Optics Letters

Quantum random number generator based on twin beams

QIANG ZHANG,[1] XIAOWEI DENG,[1] CAIXING TIAN,[1] AND XIAOLONG SU[1,2,*]

[1]*The State Key Laboratory of Quantum Optics and Quantum Optics Devices, Institute of Opto-Electronics, Shanxi University, Taiyuan 030006, China*
[2]*Collaborative Innovation Center of Extreme Optics, Shanxi University, Taiyuan, Shanxi 030006, China*
*Corresponding author: suxl@sxu.edu.cn

We produce two strings of quantum random numbers simultaneously from the intensity fluctuations of the twin beams generated by a nondegenerate optical parametric oscillator. Two strings of quantum random numbers with bit rates up to 60 Mb/s are extracted simultaneously with a suitable post-processing algorithm. By post-selecting the identical data from two raw sequences and using a suitable hash function, we also extract two strings of identical quantum random numbers. The obtained random numbers pass all NIST randomness tests. The presented scheme shows the feasibility of generating quantum random numbers from the intensity of a macroscopic optical field. © 2017 Optical Society of America

Random numbers have significant applications in science and engineering [1,2], such as cryptography, statistical analysis, numerical simulation, etc. There are two main categories of random numbers, which are pseudorandom numbers and true random numbers. Pseudorandom numbers are generated with a given software algorithm and finite length seed, which is easy to achieve a high bit rate, but powerless in some stringent occasions. True random numbers, which are generated from the measurement of unpredictable physical processes, are more secure and reliable. There are various methods to produce true random numbers, such as chaotic systems [3–5], thermal noise in electronic circuits [6], and optical noise of superluminescent LEDs [7].

True randomness is an essential part of quantum mechanics. A quantum random number generator (QRNG) exploits the inherent randomness of a quantum event to produce true random numbers. Several optical QRNGs have been proposed and demonstrated, such as QRNGs based on photon counting [8–12], attenuated pulse [13–15], phase noise of a laser [16–21], quantum vacuum fluctuations [22–26], Raman scattering [27,28], and optical parametric oscillators (OPO) [29,30]. Up to now, the QRNGs with bit rates up to Gbit/s have been achieved [19–22]. Recently, a QRNG based on the photonic integrated circuit has been demonstrated [31], which shows the feasibility of integrated QRNGs.

In the previous QRNG based on an OPO, the phase of the macroscopic field is used to produce random numbers, where two independent cavities of the same output power are used and two output fields interfered at a beam splitter [29]. In another QRNG based on an OPO, the frequency-degenerate bi-phase state of a dual-pumped degenerate OPO in a silicon nitride microresonator is used to produce random numbers [30]. The twin beams generated in the parametric down-conversion process are well known to have intensity correlation [32–37] and quantum entanglement [38–40]. In the spontaneous parametric down conversion, a nonlinear medium converts a photon at frequency ω_0 into two photons at frequency ω_s and ω_i with $\omega_0 = \omega_s + \omega_i$. In a nondegenerate optical parametric oscillator (NOPO), a type-II crystal is inserted into an optical cavity. When a NOPO is operated above threshold, the vacuum fluctuations are amplified and the continuous entangled twin beams are obtained. The vacuum fluctuations are a fundamental quantum effect, which cannot be influenced by a potential adversary. The previous QRNG based on an OPO only outputs one string of random numbers. However, based on the twin beams generated by NOPO, two strings of quantum random numbers can be produced simultaneously.

In this Letter, we demonstrate an efficient method to produce quantum random numbers from twin beams, which are generated by a NOPO. The true randomness is guaranteed by the inherited quantum fluctuations of the twin beams. The intensity fluctuations of the twin beams are measured directly by two photodetectors in the time domain, respectively. With post-processing, we extract two strings of quantum random numbers simultaneously. Based on the quantum correlation of the twin beams, we also extract two strings of identical quantum random numbers by post-selecting the identical bits from two raw sequences. Using Toeplitz hashing, the self-correlation of each individual random string is reduced. The obtained random numbers pass all NIST randomness tests.
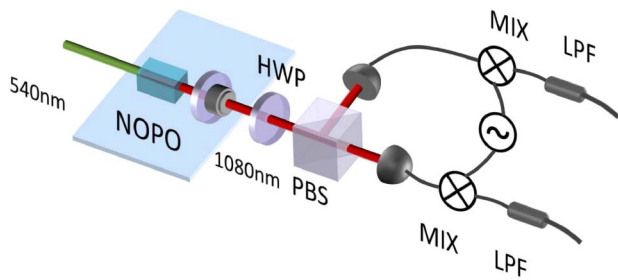
Fig. 1. Schematic of the QRNG based on twin beams. HWP: half-wave plate, PBS: polarization beam-splitter, MIX: mixer, LPF: low-pass filter.

Figure 1 shows the schematic of the QRNG based on twin beams. A continuous-wave laser beam at wavelength of 540 nm is used as the pump beam of a NOPO. The NOPO consists of an α-cut type-II KTiPO4 (KTP) crystal and a concave mirror, which is a semimonolithic configuration. The front face of the KTP is coated as the input coupler and the concave mirror with 50 mm curvature serves as the output coupler of the twin beams. The front face of the KTP crystal is coated with a transmission of 7% at 540 nm and high reflectivity at 1080 nm. The output coupler is coated with a transmission of 12.5% at 1080 nm and high reflectivity at 540 nm. The cavity length is 54 mm. In our experiment, the threshold of the NOPO is about 50 mW.

The cavity length of the NOPO is locked on the pump resonance using a feedback servo system. With a pump power of 80 mW, the NOPO emits two continuous orthogonally polarized twin beams with near degenerate wavelength at 1080 nm. The twin beams are separated by a polarization beam splitter and then focused on a pair of detectors with carefully balanced amplifications. A half-wave plate is inserted before the polarization beam splitter. When the polarization of the twin beams is rotated by an angle of 45°, the measured noise in the intensity difference is the shot noise limit (SNL). When the polarization of the twin beams is rotated by an angle of 0°, the measured noise in the intensity difference is the intensity difference spectrum of the twin beams [32].

Theoretically, the measured intensity difference spectrum of the twin beams generated by the NOPO is expressed as [32,39]

$$S(\Omega) = S_{SNL}\left(1 - \frac{\eta\xi}{1 + \Omega^2\tau_c^2}\right), \qquad (1)$$

where S_{SNL} is the shot noise limit (usually normalized to 1); Ω is the measured noise frequency; τ_c is the cavity storage time; η is the total efficiency of the detection system (including quantum efficiency of photodiode and transmission efficiency of twin beams); $\xi = T/(T + \delta)$ is the output coupling efficiency of NOPO, in which T is the transmission coefficient of the output coupling mirror; and δ is the loss of the cavity. With parameters $\Omega = 4$ MHz, $\tau_c = 0.0196$ μs, $\eta = 89.3\%$, and $\xi = 95.3\%$, the theoretical noise reduction for the intensity difference of the twin beams is 8.1 dB. Figure 2(a) shows the measured intensity difference noise of the twin beams in the frequency domain. The intensity difference noise between the twin beams is 6.3 dB below the SNL around 4 MHz, where the electronic noise is about 27.6 dB lower than the SNL. The difference between the experimentally measured squeezing and
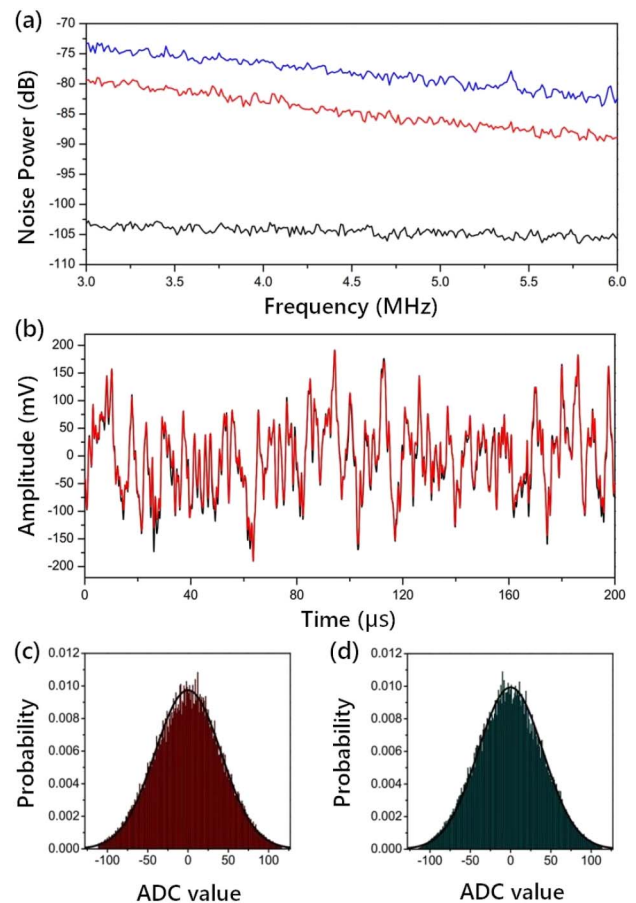
Fig. 2. (a) Measured intensity difference noise in the frequency domain. The traces from top to bottom are the SNL, intensity difference noise, and electronic noise, respectively. (b) Measured intensity noises in the time domain. Red and black lines correspond to ac outputs of the two detectors with a sample size of 2000 points, respectively. (c)–(d) Statistical histograms corresponding to each one of the measured intensity noises of the twin beams with 20,000 data digitized by the 8-bit ADC, respectively. The mathematically fitting curves are plotted with the Gaussian outlines.

the theoretical squeezing mainly comes from the imperfection of the experimental system, for example, the thermal effect of the NOPO and fluctuation of the locking system.

To exploit the correlated intensity fluctuations of the twin beams to generate quantum random numbers, we use the detected intensity noise at 4 MHz with a bandwidth of 600 kHz. The ac output of each detector is mixed with a 4 MHz sinusoid signal and then filtered by a low-pass filter whose cutoff frequency is 300 kHz [22–24]. The intensity noises of twin beams are sampled and digitized with a 8-bit ADC (National Instrument 5153) using the sampling frequency of 10 MHz. The bit rate of the produced quantum random numbers depends on the bandwidth of the NOPO, photodetector, and low-pass filter used in the measurement device. If a broadband NOPO and photodetector are used, and the photocurrents are filtered with a broadband low-pass filter, the bit rate of the produced random numbers can be increased.

Figure 2(b) shows the measured intensity noises of twin beams in the time domain. The intensity fluctuations of twin beams are correlated for about 75%. The statistical histograms

of the digitized intensity noises of twin beams are shown in Figs. 2(c) and 2(d), respectively. It is obvious that the distribution of the measured intensity noise of each one of the twin beams is Gaussian.

In order to extract quantum random numbers, we apply the min-entropy to quantify the quantum randomness of the obtained raw data. In some sense, the min-entropy is a measure of the maximum amount of information that can be obtained under a single attack [41]. The min-entropy is exploited to quantify the extraction ratio between the raw random bits and the final random bits given a probability distribution of $\{0, 1\}^N$ [42], which is evaluated as

$$H_{\min}(X) = -\log_2 \left(\max_{X \in \{0,1\}^N} \Pr[X = x] \right). \quad (2)$$

For a given sequence X, the min-entropy is determined by the sample point with maximal probability $P_{\max} = \max_{X \in \{0,1\}^N} \Pr[X = x]$.

It is reasonable to assume the quantum noise of the intensity fluctuation is perfectly random over all frequencies and independent of the classical noise. We describe the variance of the ac output voltage from the detector as $\sigma^2_{\text{total}} = \sigma^2_{\text{quant}} + \sigma^2_c$, where σ^2_{quant} and σ^2_c are variances of the quantum signal and the classical signal, respectively [22,26]. We obtain σ^2_{total} as 4768.44 mV^2 for the measured intensity noise. In our system, the classical noise mainly comes from the electronic noise of the detector, which is about 3.18 mV^2. Therefore, the quantum variance is $\sigma^2_{\text{quant}} = 4765.26$ mV^2. Assuming the quantum signal follows Gaussian distribution, the corresponding maximum probability of the raw data is $P_{\max} = 0.00993296$. Consequently, the quantum min-entropy in our experiment is estimated to be 6.65 bits per sample [20].

The raw random data cannot pass any randomness tests, mainly because the classical noise is mixed into the raw data and the sample points follow the Gaussian distribution rather than the uniform distribution [20]. In order to distill the randomness of the raw random data, we utilize the Toeplitz hashing to eliminate the classical noise and improve the statistical quality of the random numbers [20,42]. Given $m \times n$ binary Toeplitz matrix, m random bits are extracted by multiplying the Toeplitz matrix with n raw bits. We choose $m = 1024$ and $n = 1360 > 1024 \times 8/6.65 = 1232$ to obtain nearly perfect random bits. We use $n + m - 1 = 2383$ pre-stored true random bits as seed to construct the Toeplitz matrix. Therefore, two strings of quantum random numbers are extracted simultaneously at rates up to 60 Mb/s.

Based on the correlated intensity fluctuations of the twin beams, we also distill two strings of identical quantum random numbers by changing the post-processing algorithm. We post-select identical bits between the raw data sequences and discard the different bits. After post-selection, 70% of the raw random bits are selected as the input string of the Toeplitz hashing. We set $m = 1024$ and $n = 1920$ to construct the Toeplitz matrix. Consequently, two strings of identical quantum random numbers are extracted simultaneously at rates up to 29.8 Mb/s. The bit rate of identical quantum random numbers depends on the quantum correlation between intensity fluctuations of the twin beams. The higher the quantum correlation of the twin beams, the higher the bit rate; this is because there are more identical bits to be selected between two raw data sequences (less different bits are discarded).
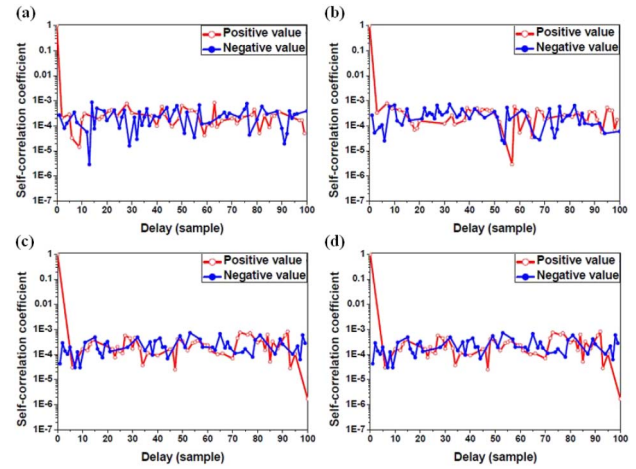
Fig. 3. Results of self-correlation analysis. Data size is 80 Mbits. (a)–(b) Results corresponding to each string of quantum random numbers with a bit rate of 60 Mb/s, respectively. (c)–(d) Results corresponding to each of two strings of identical quantum random numbers, respectively.

The self-correlation of the obtained quantum random numbers is verified by self-correlation coefficient $R(k)$ of a sequence X, which is defined as [20,26]

$$R(k) = \frac{E[(X_i - \mu)(X_{i+k} - \mu)]}{E[(X_i - \mu)^2]}, \quad (3)$$

where $E[\cdot]$ is the expected value operator, k is the sample delay, and μ is the mean of X. Figure 3 shows that the self-correlation of the random numbers is reduced by post-processing. The average values ($k \neq 0$) of Figs. 3(a)–3(d) are -3.64×10^{-5}, -1.09×10^{-5}, 3.59×10^{-6}, and 3.59×10^{-6}, respectively.

The NIST test [43] is widely considered as one of the most stringent randomness test suites. It has 15 statistical tests to evaluate the performance of a given random number generator. Each test output a p-value. A significance level α is chosen for the test. For cryptographic application, α is mostly set as 0.01. A tested sequence is considered to pass the test if the p-value $\geq \alpha$; otherwise, the sequence appears to be nonrandom. We record two random sequences of 1 Gbits. Each sequence is chopped into 1000 smaller sequences for the NIST test. Each test calculates 1000 p-values, and we use the chi-square test to calculate the final P-value, which indicates the uniformity of p-values. Figure 4 shows the results of NIST statistical test suites for two strings of quantum random numbers and two strings of identical quantum random numbers. All of them pass these tests.

In summary, we demonstrate an efficient method to produce quantum random numbers from intensity fluctuations of twin beams. The true randomness is guaranteed by the inherited quantum fluctuations of the twin beams. We observed 75% quantum correlation between the intensity fluctuations of the twin beams. The intensity fluctuations of the twin beams are measured directly by two photodetectors, and two strings of quantum random numbers with bit rates up to 60 Mb/s are extracted simultaneously with a suitable post-processing algorithm. By post-selecting identical bits, we also extract two strings of identical quantum random numbers with bit rates of 29.8 Mb/s using the same device. The obtained random numbers pass all NIST randomness tests, which confirms the randomness of the generated random numbers.
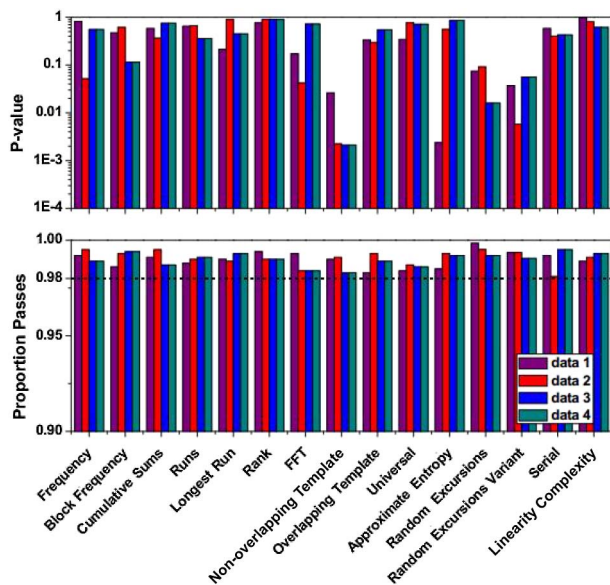
Fig. 4. Results of NIST statistical test suites. Using 1000 samples of 1 Mb and significance level $\alpha = 0.01$. For "Pass," the P-value (uniformity of p-values) should be larger than 0.0001, and the proportion should be within the range of 0.99 ± 0.0094329. For the tests that produce multiple P-values and proportions, the worst case is shown. Data 1 and data 2 show the results corresponding to each string of quantum random numbers with a bit rate of 60 Mb/s, respectively. Data 3 and data 4 show the results corresponding to each one of two strings of identical quantum random numbers, respectively.

The advantage of the presented scheme is that two strings of random numbers can be extracted simultaneously, especially two strings of identical quantum random numbers which are extracted by post-selection. The bit rate of the quantum random numbers produced in this scheme is limited by the bandwidth of the preparation and measurement systems of the twin beams. To obtain a higher bit rate of two strings of identical quantum random numbers, twin beams with higher quantum correlation are required, which means that lower intracavity losses of NOPO and a detection system with better performance are required. It has been shown that twin beams can be generated by an on-chip monolithically integrated optical parametric oscillator [44], which shows the possibility of an integrated QRNG based on twin beams. Our work also shows the possibility to use entangled lights to generate quantum random numbers.

REFERENCES

1. M. Herrero-Collantes and J. C. Garcia-Escartin, "Quantum random number generators," arXiv: 1604.03304v1 [quant-ph] (2016).
2. X. Ma, X. Yuan, Z. Cao, B. Qi, and Z. Zhang, "Quantum random number generation," arXiv: 1510.08957v2 [quant-ph] (2016).
3. X.-Z. Li and S.-C. Chan, Opt. Lett. **37**, 2163 (2012).
4. P. Li, Y. Sun, X. Liu, X. Yi, J. Zhang, X. Guo, Y. Guo, and Y. Wang, Opt. Lett. **41**, 3347 (2016).
5. T. Butler, C. Durkan, D. Goulding, S. Slepneva, B. Kelleher, S. P. Hegarty, and G. Huyet, Opt. Lett. **41**, 388 (2016).
6. C. S. Petrie and J. A. Connelly, IEEE Trans. Circuits Syst. I **47**, 615 (2000).
7. X. Li, A. B. Cohen, T. E. Murphy, and R. Roy, Opt. Lett. **36**, 1020 (2011).
8. J. G. Rarity, P. C. M. Owens, and P. R. Tapster, J. Mod. Opt. **41**, 2435 (1994).
9. T. Jennewein, U. Achleitner, G. Weihs, H. Weinfurter, and A. Zeilinger, Rev. Sci. Instrum. **71**, 1675 (2000).
10. A. Stefanov, N. Gisin, O. Guinnard, L. Guinnard, and H. Zbinden, J. Mod. Opt. **47**, 595 (2000).
11. S. Pironio, A. Acn, S. Massar, A. B. de la Giroday, D. N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T. A. Manning, and C. Monroe, Nature **464**, 1021 (2010).
12. J. F. Dynes, Z. L. Yuan, A. W. Sharpe, and A. J. Shields, Appl. Phys. Lett. **93**, 031109 (2008).
13. W. Wei and H. Guo, Opt. Lett. **34**, 1876 (2009).
14. Z. Bisadi, A. Meneghetti, G. Fontana, G. Pucker, P. Bettotti, and L. Pavesi, Proc. SPIE **9520**, 952004 (2015).
15. M. Stipčević and R. Ursin, Sci. Rep. **5**, 10214 (2015).
16. H. Guo, W. Tang, Y. Liu, and W. Wei, Phys. Rev. E **81**, 051137 (2010).
17. B. Qi, Y.-M. Chi, H.-K. Lo, and L. Qian, Opt. Lett. **35**, 312 (2010).
18. H. Zhou, X. Yuan, and X. Ma, Phys. Rev. A **91**, 062316 (2015).
19. Y. Zhu, Y. Lu, J. Zhu, and G. Zeng, Int. J. Quantum Inf. **9**, 1113 (2011).
20. F. Xu, B. Qi, X. Ma, H. Xu, H. Zheng, and H.-K. Lo, Opt. Express **20**, 12366 (2012).
21. Y.-Q. Nie, L. Huang, Y. Liu, F. Payne, J. Zhang, and J.-W. Pan, Rev. Sci. Instrum. **86**, 063105 (2015).
22. T. Symul, S. M. Assad, and P. K. Lam, Appl. Phys. Lett. **98**, 231103 (2011).
23. Y. Shen, L. Tian, and H. Zou, Phys. Rev. A **81**, 063814 (2010).
24. C. Gabriel, C. Wittmann, D. Sych, R. Dong, W. Mauerer, U. L. Andersen, C. Marquardt, and G. Leuchs, Nat. Photonics **4**, 711 (2010).
25. Y. Zhu, G. He, and G. Zeng, Int. J. Quantum Inf. **10**, 1250012 (2012).
26. Y. Shi, B. Chng, and C. Kurtsiefer, Appl. Phys. Lett. **109**, 041101 (2016).
27. P. J. Bustard, D. Moffatt, R. Lausten, G. Wu, I. A. Walmsley, and B. J. Sussman, Opt. Express **19**, 25173 (2011).
28. P. J. Bustard, D. G. England, J. Nunn, D. Moffatt, M. Spanner, R. Lausten, and B. J. Sussman, Opt. Express **21**, 29350 (2013).
29. A. Marandi, N. C. Leindecker, K. L. Vodopyanov, and R. L. Byer, Opt. Express **20**, 19322 (2012).
30. Y. Okawachi, M. Yu, K. Luke, D. O. Carvalho, M. Lipson, and A. L. Gaeta, Opt. Lett. **41**, 4194 (2016).
31. C. Abellan, W. Amaya, D. Domenech, P. Muñoz, J. Capmany, S. Longhi, M. W. Mitchell, and V. Pruneri, Optica **3**, 989 (2016).
32. A. Heidmann, R. J. Horowicz, S. Reynaud, E. Giacobino, C. Fabre, and G. Camy, Phys. Rev. Lett. **59**, 2555 (1987).
33. P. H. Souto Ribeiro, C. Schwob, A. Matre, and C. Fabre, Opt. Lett. **22**, 1893 (1997).
34. H. Wang, Y. Zhang, Q. Pan, H. Su, A. Porzio, C. Xie, and K. Peng, Phys. Rev. Lett. **82**, 1414 (1999).
35. J. Gao, F. Cui, C. Xue, C. Xie, and K. Peng, Opt. Lett. **23**, 870 (1998).
36. J. Laurat, T. Coudreau, N. Treps, A. Matre, and C. Fabre, Phys. Rev. Lett. **91**, 213601 (2003).
37. Y. Zhang, K. Kasai, and M. Watanabe, Opt. Express **11**, 14 (2003).
38. A. S. Villar, L. S. Cruz, K. N. Cassemiro, M. Martinelli, and P. Nussenzveig, Phys. Rev. Lett. **95**, 243603 (2005).
39. X. Su, A. Tan, X. Jia, Q. Pan, C. Xie, and K. Peng, Opt. Lett. **31**, 1133 (2006).
40. J. Jing, J. Zhang, Y. Yan, F. Zhao, C. Xie, and K. Peng, Phys. Rev. Lett. **90**, 167903 (2003).
41. M. A. Wayne and P. G. Kwiat, Opt. Express **18**, 9351 (2010).
42. X.-G. Zhang, Y.-Q. Nie, H. Zhou, H. Liang, X. Ma, J. Zhang, and J.-W. Pan, Rev. Sci. Instrum. **87**, 076102 (2016).
43. A. Rukhin, J. Soto, J. Nechvatal, M. Smid, E. Barker, S. Leigh, M. Levenson, M. Vangel, D. Banks, A. Heckert, J. Dray, and S. Vo, *A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications* (NIST, 2010) https://www.nist.gov/node/562666.
44. A. Dutt, K. Luke, S. Manipatruni, A. L. Gaeta, P. Nussenzveig, and M. Lipson, Phys. Rev. Appl. **3**, 044005 (2015).