Optics Letters

Quantum random number generator using a microresonator-based Kerr oscillator

Yoshitomo Okawachi,[1,*,†] Mengjie Yu,[1,2,†] Kevin Luke,[2] Daniel O. Carvalho,[2,3] Michal Lipson,[4] and Alexander L. Gaeta[1]

[1]Department of Applied Physics and Applied Mathematics, Columbia University, New York, New York 10027, USA
[2]School of Electrical and Computer Engineering, Cornell University, Ithaca, New York 14853, USA
[3]Currently at São Paulo State University (UNESP), São João da Boa Vista, Brazil
[4]Department of Electrical Engineering, Columbia University, New York, New York 10027, USA
*Corresponding author: y.okawachi@columbia.edu

Received 18 July 2016; accepted 16 August 2016; posted 19 August 2016 (Doc. ID 270738); published 8 September 2016

We demonstrate an all-optical quantum random number generator using a dual-pumped degenerate optical parametric oscillator in a silicon nitride microresonator. The frequency-degenerate bi-phase state output is realized using parametric four-wave mixing in the normal group-velocity dispersion regime with two nondegenerate pumps. We achieve a random number generation rate of 2 MHz and verify the randomness of our output using the National Institute of Standards and Technology Statistical Test Suite. The scheme offers potential for a chip-scale random number generator with gigahertz generation rates and no postprocessing.

OCIS codes: (190.4380) Nonlinear optics, four-wave mixing; (190.4970) Parametric oscillators and amplifiers; (190.4390) Nonlinear optics, integrated optics.

http://dx.doi.org/10.1364/OL.41.004194

Random number generators (RNGs) are a critical component for applications in cryptography, Monte Carlo simulations, gaming, statistical sampling, and quantitative finance [1–5]. For many of these applications, it is desirable to have a RNG that is low cost and has high generation rates, while maintaining a high degree of randomness [6]. While there are many algorithms in computer programming for random number generation [7], these generate pseudo-random numbers that are not truly indeterministic. Recently, there have been significant investigations of RNGs based on quantum mechanical systems [6,8–21], where the phenomena is intrinsically random. However, many of the quantum RNGs require extensive modeling of the quantum process for significant postprocessing or characterization of the source and readout device in order to ensure that the output is truly random, which significantly limits the generation rate.

Alternatively, over the past several years, there has been investigations on using degenerate optical parametric oscillators (OPOs) based on the second-order nonlinearity $\chi^{(2)}$ for random number generation [22]. Degenerate OPO's undergo a non-equilibrium phase transitions at the oscillation threshold. Here, the generated signal field locks to the pump field with two possible phase states which are offset by π. Marandi, *et al.* [22] used such bi-phase state generation in a pulsed OPO system to realize an all-optical RNG. Since oscillation is initiated from quantum noise, the system is intrinsically unbiased, and only requires the detection of strong, classical signals with no postprocessing, which greatly reduces complexity and required computational overhead. In addition, this bi-phase state generation can be used to create a network of coupled OPO's to realize a novel form of coherent computing by simulating the classical Ising model, [23–26]. Here, the bi-phase state is analogous to a binary spin system, and more complex phase-locked states can be achieved with a network of coupled OPO's, which corresponds to finding the ground state of the Ising model.

In a similar fashion $\chi^{(3)}$-based degenerate OPO's can be utilized to generate these random bi-phase states [27,28]. Here, parametric oscillation relies on parametric four-wave mixing (FWM) interactions, and two frequency non-degenerate pumps are required to achieve degenerate signal/idler pair generation [29,30]. Efficient parametric FWM is dictated by the phase matching condition $\Delta\phi = \phi_1 + \phi_2 - 2\phi_3$, where ϕ_1 and ϕ_2 are the phases of the two pumps and ϕ_3 is the phase of the generated signal/idler pair. The same phase-matching conditions are maintained for a π phase shift in the generated field, indicating that the OPO can operate with two possible phase conditions that are offset by π, and recent work has demonstrated the bi-phase state in a 1.05-km-long optical fiber cavity [28]. Using a $\chi^{(3)}$ nonlinear process enables integration with silicon-based photonics technology. The silicon nitride (Si_3N_4) platform is particularly favorable for operation in the near-infrared regime since it is CMOS-process compatible, has low linear and nonlinear losses, has a high $\chi^{(3)}$ nonlinearity, and allows for dispersion engineering, which is crucial for efficient FWM processes [31]. Si_3N_4 is a highly promising platform for nonlinear photonics, with significant work done recently in the context of FWM-based frequency comb generation [32–36] and supercontinuum generation [37–42].

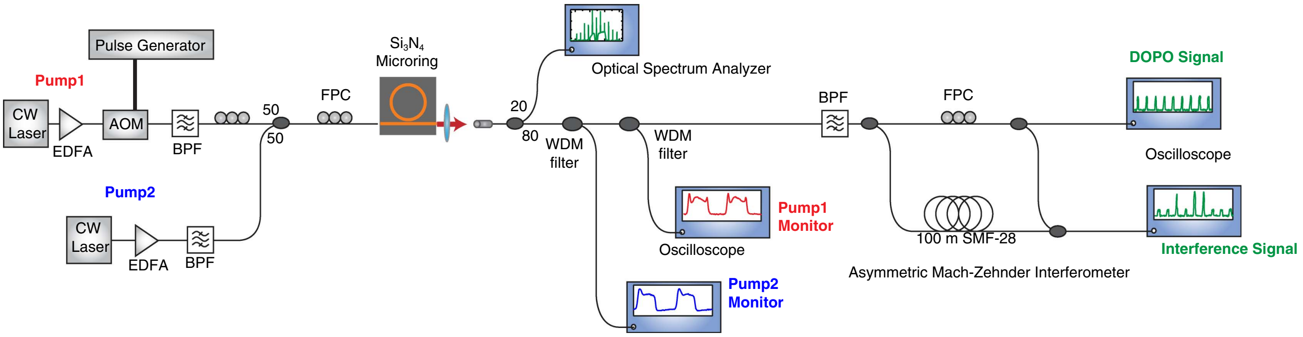

Fig. 1. Experimental setup for RNG using degenerate OPO. The power of pump1 is modulated using an acousto-optic modulator (AOM). Both pumps are monitored using a photodiode and an oscilloscope to ensure that they are tuned to the microresonator resonance. The generated bi-phase state is characterized using an asymmetric Mach–Zehnder interferometer. EDFA, erbium-doped fiber amplifier; BPF, bandpass filter; WDM, wavelength division multiplexing.

In this paper, we experimentally demonstrate an all-optical quantum RNG using a dual-pumped degenerate OPO in a Si_3N_4 microresonator. We demonstrate a generation rate of 2 MHz by amplitude modulating one of the two pump lasers. We verify the generation of the bi-phase state when parametric oscillation is achieved using an asymmetric Mach–Zehnder interferometer. In addition, to verify the randomness of our RNG output, we analyze our sample bits using statistical tests developed by the National Institute of Standards and Technology (NIST).

In order to realize degenerate parametric oscillation in Si_3N_4 microresonators, we require a dual-pump configuration and operation in the normal group-velocity dispersion (GVD) regime [27]. Figure 1 shows our experimental setup. The microresonator has an effective cross section of 690 nm × 1300 nm and a free spectral range (FSR) of 200 GHz. The two pumps are offset by frequency $\pm\delta$ from the degeneracy point [Fig. 2(a)]. For maximum parametric gain at the degeneracy point, we require the dispersion length $L_D = 1/\delta^2|\beta_2|$ to be larger than the nonlinear length $L_{\text{NL}} = 1/2\gamma P$, where β_2 is the GVD parameter, γ is the nonlinear parameter, and P is the power for each pump [Fig. 2(b)]. The pumps are generated by amplifying two single-frequency tunable lasers using erbium-doped fiber amplifiers. The wavelengths of pump1 and pump2 are set to 1557.8 and 1545.2 nm, respectively, which correspond to 4 × FSRs from the frequency degeneracy point. We modulate the amplitude of pump1 using an acousto-optic modulator (AOM) driven with 250 ns pulses at a repetition rate of 2 MHz. The pulse duration, amplitude, and DC offset of the modulation is chosen to take into account thermal effects in the resonator to optimize OPO generation. The two pumps are combined and coupled into a Si_3N_4 microresonator, and the polarization is set to quasi-TM, for which the normal GVD allows for the necessary phase-matching conditions needed for efficient parametric gain. The total pump power in the bus waveguide is 128 mW. To achieve threshold in the OPO, we tune the frequency of each pump laser into its respective cavity resonance, taking into account the thermal shift of the resonance due to pump power build-up. We monitor the pump transmission to ensure that both are in-resonance.

To verify the generation of bi-phase states, we measure the phase of the generated train of OPO pulses using a bandpass filter to transmit only the degenerate OPO signal and send it to an asymmetric Mach–Zehnder interferometer. We use a 100 m length of SMF-28 in one arm to characterize the relative phase between adjacent bits. A polarization controller is inserted in one path to optimize the interference signal. Constructive interference and destructive interference correspond to a relative phase of 0 and π, respectively. As shown in Fig. 1, a 50/50 splitter is inserted in one arm of the interferometer to measure the amplitude of the degenerate OPO signal.

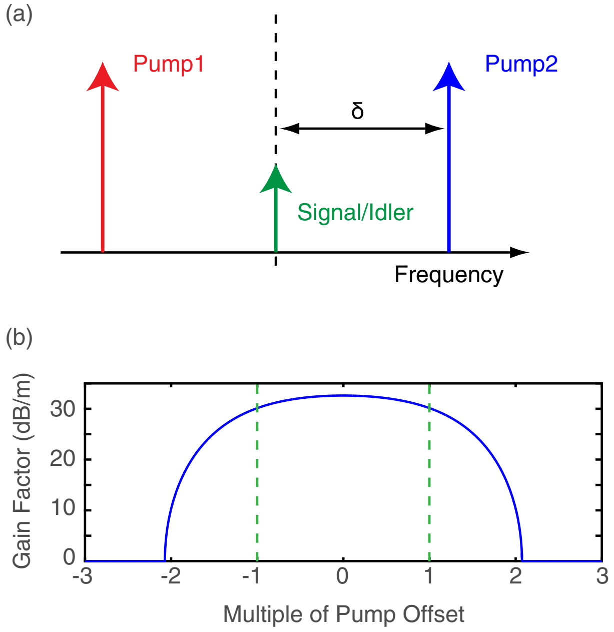

Fig. 2. (a) Scheme for degenerate OPO. For degenerate operation, two pumps that are frequency offset by δ are sent into a Si_3N_4 microresonator to generate a signal/idler pair at the degeneracy point via FWM in the normal GVD regme. (b) Parametric gain profile for two nondegenerate pumps. The pump separation is 12.6 nm, and the degeneracy wavelength is 1551.5 nm. The GVD ($\beta_2 = 195\ \text{ps}^2/\text{km}$) and nonlinear parameter ($\gamma = 0.94\ \text{W}^{-1}\ \text{m}^{-1}$) are based on a Si_3N_4 waveguide with a cross section of 690 nm × 1300 nm. The pump positions are denoted by dashed green lines. The ratio between dispersion length L_D and nonlinear length L_{NL} is 3.3.

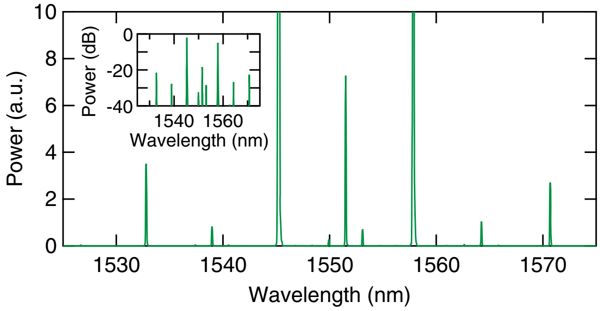

Fig. 3. Optical spectrum of degenerate OPO in a Si_3N_4 microresonator. The inset shows the spectrum in dB. The pumps are located 4 × FSRs from the degeneracy point.

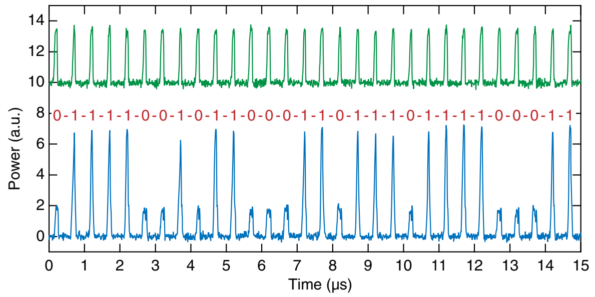

Fig. 5. Temporal measurement of degenerate OPO RNG. Plot shows the time trace of the OPO output (green) and the corresponding output from the asymmetric Mach–Zehnder interferometer (blue).

Figure 3 shows the generated OPO spectrum in which the degenerate signal is generated at 1551.5 nm. Figure 4 shows the time-domain measurement. The electrical modulation signal used to drive the AOM is shown in black, and the detected pump1 and the degenerate OPO output are shown in red and green, respectively. The structure visible in the temporal profile of the pump pulses is the result of thermal effects due to power build-up of both pumps in the microresonator that causes the resonances to shift. We observe that the OPO signal is generated toward the end of the pump pulse. Due to thermal effects in the microresonator, we adjust the modulation frequency, pulse duration, and amplitude of pump1 to maximize the efficiency of the generation process while ensuring that the OPO signal is extinguished each time pump1 reaches its minimum amplitude. The stability of the output can be further improved by stabilizing the pump laser frequency and the pump power fluctuations.

To verify the generation of a bi-phase state, we simultaneously measure the degenerate OPO output (green) and the interferometer output (blue) to characterize the phase of our system (Fig. 5). The 100 m pathlength difference between the two arms of the interferometer allows for characterization of the relative phase between adjacent bits. In the interferometer output (blue), the maximum and minimum amplitude correspond to constructive and destruction interference, respectively, between adjacent bits. Thus a change in amplitude in the temporal pulse train corresponds to a π phase shift in the binary sequence. The simultaneous measurement of the OPO output sans interferometer effectively acts as a clock signal and ensures that the minimum amplitude is due to destructive interference and not due to the absence of an OPO signal. This verification of bi-phase state generation is critical for random number generation and a significant step toward the realization of a chip-based photonic Ising machine using coupled OPOs.

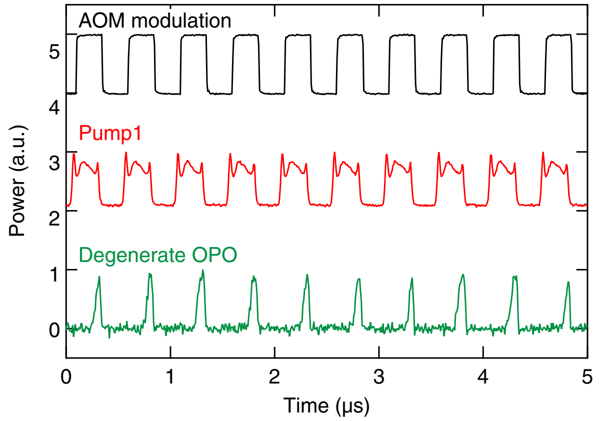

Fig. 4. Temporal characterization of degenerate OPO. Plot shows the modulation signal for the AOM (black), the measured pump1 (red), and degenerate OPO output (green). The generation rate of our system is 2 MHz.

Finally, we test the randomness of our degenerate OPO output. We use the NIST Statistical Test Suite (NIST STS-2.1.2), which is comprised of a series of statistical hypothetical tests designed to detect non-randomness and assess proportion and uniformity [43]. Our sample consists of 217,000 bits, which are divided into 100 samples each with 2170 bits. The test results are shown in Fig. 6. The Final Analysis Report from the NIST STS indicates that the minimum pass rate for each statistical test is 96%, indicating that our sample passes each of the NIST statistical tests. Our current generation rate is 2 MHz and is largely dependent on the cavity lifetime of the microresonator [22], pump power, and the thermal effect in Si_3N_4.

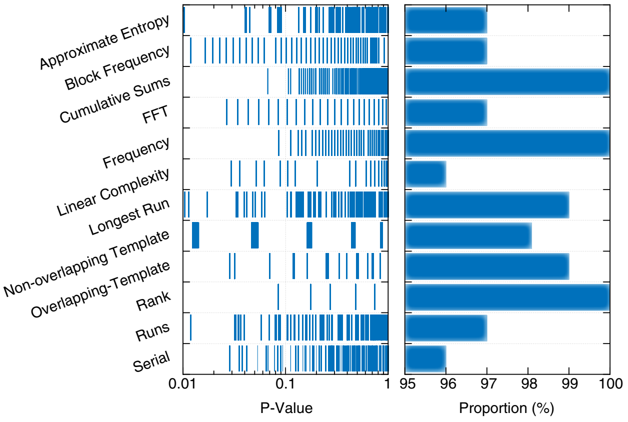

Fig. 6. Test results for randomness using the NIST Statistical Test Suite (NIST STS-2.1.2). Our sample consists of 100 sets of 2170 bits. The p-value indicates the probability that a perfect RNG would output a sequence that is less random than the test sequence [43]. The proportion indicates the percentage of sequences that pass the tests with a significance level $\alpha > 0.01$, which indicates the upper bound for the probability of incorrectly rejecting the null hypothesis. From the NIST standard, the minimum pass rate for our sample size is 96 percentile.

We believe that our RNG can operate at generation rates approaching 1 GHz with appropriate resonator design, including dispersion engineering, cavity FSR, quality factor, and athermal operation [44].

In conclusion, we demonstrate an all-optical quantum RNG based on a degenerate OPO using dual-pumped FWM in a Si_3N_4 microresonator. We show a generation rate of 2 MHz and verify the randomness of our output using the NIST statistical tests. Since our OPO system operates above threshold, our scheme involves detection of classical signals, which significantly simplifies the complexity of the system. Furthermore, we believe our generation rate can be significantly increased beyond 1 GHz while maintaining a compact footprint by using a system of time-multiplexed OPOs. Our scheme offers promise for realizing a compact chip-scale RNG with potential applications including cryptography, computer programming, and Monte Carlo simulations.

Funding. Defense Advanced Research Projects Agency (DARPA) (W31P4Q-15-1-0015); Air Force Office of Scientific Research (AFOSR) (FA9550-15-1-0303); National Science Foundation (NSF) (ECS-0335765, ECCS-1306035).

Acknowledgment. This work was performed in part at the Cornell Nano-Scale Facility, a member of the National Nanotechnology Infrastructure Network, which is supported by the NSF. We thank H. Zhang, A. Dutt, A. Klenner, and J. Jang for useful discussions.

[†]These authors contributed equally to this work.

REFERENCES

1. A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
2. A. J. Alspector, J. Gupta, and R. B. Allen, *Advances in Neural Information Processing* (AIP, 1988).
3. S. Banks, P. Beadling, and A. Ferencz, in *International Conference on Reconfigurable, Computing and FPGAs, RECONFIG '08* (IEEE, 2008), pp. 271–276.
4. C. Kenny, "Random number generators: an evaluation and comparison of random.org and some commonly used generators," Trinity College Dublin Management Science and Information Systems Studies Report (Trinity College Dublin, 2005), https://www.random.org/analysis/Analysis2005.pdf.
5. C. H. Bennet, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, J. Cryptology **5**, 3 (1992).
6. D. E. Knuth, *Seminumerical Algorithms* Vol. **2** of Art of Computer Programming (Addison-Wesley, 2014).
7. X. Ma, X. Yuan, Z. Cao, B. Qi, and Z. Zhang, NPJ Quantum Inf. **2**, 16021 (2016).
8. T. Jennewein, U. Achleitner, G. Weihs, H. Weinfurter, and A. Zeilinger, Rev. Sci. Instrum. **71**, 1675 (2000).
9. M. Fiorentino, C. Santori, S. M. Spillane, R. G. Beausoleil, and W. J. Munro, Phys. Rev. A **75**, 032334 (2007).
10. M. A. Wayne and P. G. Kwiat, Opt. Express **18**, 9351 (2010).
11. S. Pironio, A. Acin, 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. C. Gabriel, C. Wittmann, D. Sych, R. Dong, W. Mauerer, U. L. Andersen, C. Marquardt, and G. Leuchs, Nat. Photonics **4**, 711 (2010).
13. H. Guo, W. Tang, Y. Liu, and W. Wei, Phys. Rev. E **81**, 051137 (2010).
14. M. Jofre, M. Curty, F. Steinlechner, G. Anzolin, J. P. Torres, M. W. Mitchell, and V. Pruneri, Opt. Express **19**, 20665 (2011).
15. M. Wahl, M. Leifgen, M. Berlin, T. Rhlicke, H. Rahn, and O. Benson, Appl. Phys. Lett. **98**, 171105 (2011).
16. T. Symul, S. M. Assad, and P. K. Lam, Appl. Phys. Lett. **98**, 231103 (2011).
17. P. J. Bustard, D. Moffatt, R. Lausten, G. Wu, I. A. Walmsley, and B. J. Sussman, Opt. Express **19**, 25173 (2011).
18. Y. Jian, M. Ren, E. Wu, G. Wu, and H. Zeng, Rev. Sci. Instrum. **82**, 073109 (2011).
19. C. Abellán, W. Amaya, M. Jofre, M. Curty, A. Acín, J. Capmany, V. Pruneri, and M. W. Mitchell, Opt. Express **22**, 1645 (2014).
20. M. Stipčević and R. Ursin, Sci. Rep. **5**, 10214 (2015).
21. Z. Cao, H. Zhou, X. Yuan, and X. Ma, Phys. Rev. X **6**, 011020 (2016).
22. A. Marandi, N. C. Leindecker, K. L. Vodopyanov, and R. L. Byer, Opt. Express **20**, 19322 (2012).
23. E. Ising, Z. Phys. **31**, 253 (1925).
24. Z. Wang, A. Marandi, K. Wen, R. L. Byer, and Y. Yamamoto, Phys. Rev. A **88**, 063853 (2013).
25. A. Marandi, Z. Wang, K. Takata, R. L. Byer, and Y. Yamamoto, Nat. Photonics **8**, 937 (2014).
26. K. Takata, A. Marandi, R. Hamerly, Y. Haribara, D. Maruo, S. Tamate, H. Sakaguchi, S. Utsunomiya, and Y. Yamamoto, "A 16-bit coherent Ising machine for one-dimensional ring and cubic graph problems," arXiv:1605.03847 (2016).
27. Y. Okawachi, M. Yu, K. Luke, D. O. Carvalho, S. Ramelow, A. Farsi, M. Lipson, and A. L. Gaeta, Opt. Lett. **40**, 5267 (2015).
28. T. Inagaki, K. Inaba, R. Maherly, K. Inoue, Y. Yamamoto, and H. Takesue, Nat. Photonics **10**, 415 (2016).
29. S. Radic and C. J. McKinstrie, Opt. Fiber Technol. **9**, 7 (2003).
30. S. K. Turitsyn, A. E. Bednyakova, M. P. Fedoruk, S. B. Papernyi, and W. R. L. Clements, Nat. Photonics **9**, 608 (2015).
31. D. J. Moss, R. Morandotti, A. L. Gaeta, and M. Lipson, Nat. Photonics **7**, 597 (2013).
32. Y. Okawachi, K. Saha, J. S. Levy, Y. H. Wen, M. Lipson, and A. L. Gaeta, Opt. Lett. **36**, 3398 (2011).
33. F. Ferdous, H. Miao, D. E. Leaird, K. Srinivasan, J. Wang, L. Chen, L. T. Varghese, and A. M. Weiner, Nat. Photonics **5**, 770 (2011).
34. S.-W. Huang, H. Zhou, J. Yang, J. F. McMillan, A. Matsko, M. Yu, D.-L. Kwong, L. Maleki, and C. W. Wong, Phys. Rev. Lett. **114**, 053901 (2015).
35. V. Brasch, M. Geiselmann, T. Herr, G. Lihachev, M. H. P. Pfeiffer, M. L. Gorodetsky, and T. J. Kippenberg, Science **351**, 357 (2016).
36. C. Joshi, J. K. Jang, K. Luke, X. Ji, S. A. Miller, A. Klenner, Y. Okawachi, M. Lipson, and A. L. Gaeta, Opt. Lett. **41**, 2565 (2016).
37. R. Halir, Y. Okawachi, J. S. Levy, M. A. Foster, M. Lipson, and A. L. Gaeta, Opt. Lett. **37**, 1685 (2012).
38. H. Zhao, B. Kuyken, S. Clemmen, F. Leo, A. Subramanian, A. Dhakal, P. Helin, S. Severi, E. Brainis, G. Roelkens, and R. Baets, Opt. Lett. **40**, 2177 (2015).
39. J. P. Epping, T. Hellwig, M. Hoekman, R. Mateman, A. Leinse, R. G. Heideman, A. van Rees, P. J. M. van der Slot, C. J. Lee, C. Fallnich, and K.-J. Boller, Opt. Express **23**, 19596 (2015).
40. A. S. Mayer, A. Klenner, A. R. Johnson, K. Luke, M. R. E. Lamont, Y. Okawachi, M. Lipson, A. L. Gaeta, and U. Keller, Opt. Express **23**, 15440 (2015).
41. A. R. Johnson, A. S. Mayer, A. Klenner, K. Luke, E. S. Lamb, M. R. E. Lamont, C. Joshi, Y. Okawachi, F. W. Wise, M. Lipson, U. Keller, and A. L. Gaeta, Opt. Lett. **40**, 5117 (2015).
42. A. Klenner, A. S. Mayer, A. R. Johnson, K. Luke, M. R. E. Lamont, Y. Okawachi, M. Lipson, A. L. Gaeta, and U. Keller, Opt. Express **24**, 11043 (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, *NIST Special Publication 800-22, Rev. 1-a* (NIST, 2010).
44. F. Qiu, A. M. Spring, F. Yu, and S. Yokoyama, Appl. Phys. Lett. **102**, 051106 (2013).