Random number generation using spontaneous symmetry breaking in a Kerr resonator

Liam Quinn, Gang Xu, Yiqing Xu, Zongda Li, Julien Fatome, Stuart Murdoch, Stéphane Coen, Miro Erkintalo

Random number generation using spontaneous symmetry breaking in a Kerr resonator

Liam Quinn[1, 2, *], Gang Xu[1, 2], Yiqing Xu[1, 2], Zongda Li[1, 2], Julien Fatome[3], Stuart G. Murdoch[1, 2], Stéphane Coen[1, 2], and Miro Erkintalo[1, 2]

[1] *Physics Department, The University of Auckland, Auckland 1142, New Zealand*
[2] *The Dodd-Walls Centre for Photonic and Quantum Technologies*
[3] *Laboratoire Interdisciplinaire Carnot de Bourgogne, UMR 6303 CNRS-Université de Bourgogne, Dijon, France*
[*] *Corresponding author: liam.quinn@auckland.ac.nz*

We experimentally demonstrate an all-optical random number generator based on spontaneous symmetry breaking in a coherently-driven Kerr resonator. Random bit sequences are generated by repeatedly tuning a control parameter across a symmetry-breaking bifurcation that enacts random selection between two possible steady-states of the system. Experiments are performed in a fibre ring resonator, where the two symmetry-broken steady-states are associated with orthogonal polarization modes. Detrimental biases due to system asymmetries are completely suppressed by leveraging a recently-discovered self-symmetrization phenomenon that ensures the symmetry breaking dynamics act as an unbiased coin toss, with a genuinely random selection between the two available steady-states. We optically generate bits at a rate of over 3 MHz without post-processing and verify their randomness using the National Institute of Standards and Technology and Dieharder statistical test suites.

Coherently-driven nonlinear resonators have attracted significant attention over the last decade due to their potential applications, including the generation of optical frequency combs [1–3], as well as the rich physics and dynamics they exhibit, involving phenomena such as dissipative solitons and complex phase transitions [4–6]. In this context, one universal nonlinear phenomenon that has stimulated particular recent interest is spontaneous symmetry breaking (SSB), with pioneering experimental observations reported in monolithic microresonators [7–9], macroscopic fibre ring resonators [10, 11], and coupled-cavities [12]. SSB refers to the ubiquitous process whereby a physical system in a symmetric state loses its symmetry in favour of two asymmetric states – a phenomenon that can be accessed by tuning a control parameter across a bifurcation point. In the context of systems involving a single resonator [7–11], SSB has been observed between two counter-propagating fields [7–9], as well as between co-propagating orthogonal polarization modes [10, 11], with the detuning between the driving laser and a cavity resonance (or the power of that laser) acting as the control parameter [8, 10]. In each case, slight power deviations between the two competing fields circulating in the cavity are magnified over consecutive roundtrips, leading to the selection of one of the possible asymmetric states [7, 13]. Under perfectly symmetric operating conditions, the selection enacted by SSB is completely random, alluding to the possibility of using the phenomenon for the generation of random numbers that are critical for various applications, including cryptography and security [14, 15]. Unfortunately, in practice, this prospect is typically prohibited as a result of the sensitivity of SSB to residual asymmetries, which leads to a statistical preference towards one of the states, thus preventing truly random selection upon symmetry-breaking [10, 16].

Remarkably, a phenomenon was recently discovered that can completely eliminate the impact of asymmetries on polarization SSB dynamics in fibre ring resonators. Specifically, it was shown in [17] that the implementation of a $\pi-$phase shift between two orthogonal polarization modes of the resonator resulted in a period-2 (P2) switching behaviour between two polarization modes in the cavity, somewhat similar to the period doubling regime used in bulk optical parametric oscillators [18, 19]. This periodic switching leads to a natural 'self-symmetrization' of the system, as asymmetries are averaged out over two roundtrips. While the results in [17] presented convincing evidence of the randomness of the SSB process and highlighted the potential for random number generation, the system was not yet optimised for fast random number generation and lacked a thorough analysis of the statistical properties of the generated bit sequence.

Here we report on a comprehensive experimental study of random number generation based on SSB in a coherently-driven Kerr resonator under conditions of self-symmetrized operation. Building upon the experiment reported in [17], we construct an optimised setup that allows us to generate random optical bits at rates exceeding 3 MHz without post-processing by repeatedly scanning the cavity detuning across the SSB bifurcation point. We judiciously demonstrate the randomness of the system by showing that the generated sequences pass all pertinent tests from the National Institute of Standards and Technology and Dieharder Statistical Test Suites [20, 21]. Our scheme offers

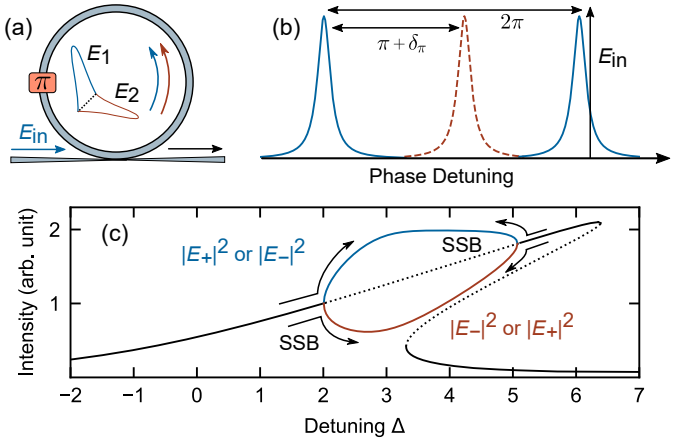

Fig. 1. **(a)** Schematic illustration of a passive, coherently-driven Kerr resonator supporting two orthogonal polarization modes. Only one mode is driven, and a π phase-defect separates the resonances of the two cavity modes E_1 and E_2. **(b)** Cavity resonances for the two principal polarization modes E_1 and E_2. E_{in} corresponds to the driving field, while δ_π describes the deviation of the mode resonance separation from π. **(c)** Bifurcation diagram, showing the intensities of the intracavity steady-states in the circular basis. The solutions are symmetric ($|E_+|^2 = |E_-|^2$) for small and large detunings, but become asymmetric via SSB. Solid (dashed) curves represent stable (unstable) solutions.

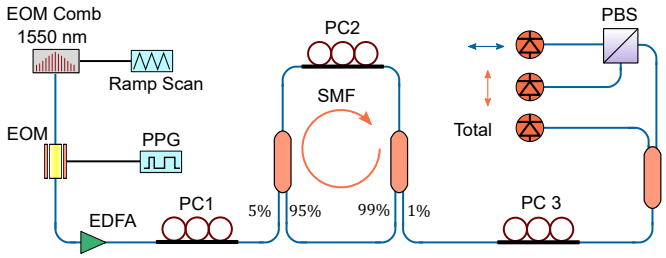

Fig. 2. Experimental setup. PPG: pulse pattern generator, PC: polarization controller, EDFA: erbium doped fibre amplifier, PBS: polarization beam splitter, EOM: Electro-optic modulator, SMF: Single mode fibre.

future potential for random number generation with GHz repetition rates and requires no post-processing. Moreover, thanks to its all-optical nature, our scheme could enable random number generation with improved speed and energy efficiency compared to current state-of-the-art systems [19, 22, 23]. In addition, the fact that our scheme is an all-fiber system operating at 1550 nm makes it an excellent candidate for integration with other optical devices. By demonstrating the true randomness of the SSB process, our results also underline the potential of the self-symmetrized mechanism for the realization of a novel coherent Ising [24–26] or Potts machine [27].

We first briefly summarise the physics of the self-symmetrized SSB scheme that underpins our experiments [17]. To this end, Fig. 1(a) shows a conceptual illustration of our SSB-based random number generator (RNG). The system is built around a passive, coherently-driven nonlinear Kerr resonator supporting two principal orthogonal polarization modes (E_1 and E_2) – defined as polarization modes that map back to themselves at the end of each roundtrip. Only one of the principal modes is driven, and the cavity resonances corresponding to the two modes are offset by a phase-detuning of approximately π, realized via a birefringent defect (polarization controller) within the cavity. To understand the dynamics of the system, we consider the intracavity field evolution in the circular polarization basis, defining the left- and right-circular polarization components as $E_\pm = (E_1 \pm iE_2)/\sqrt{2}$. As a result of the π-phase shift between the two cavity modes, the sign of one of these components (e.g. E_2) becomes inverted relative to the other at each roundtrip $E_2 \longrightarrow E_2 e^{i\pi} = -E_2$. This alternating effect leads to a periodic swapping of the circular polarization projections such that, at the end of each roundtrip, E_+ and E_- swap values. Over two roundtrips, each circular polarization component returns to their original value, and it was shown in [17] that the evolution of the components, when averaged over two roundtrips, obeys coupled Lugiato-Lefever -like mean-field equations, which are well-known to display SSB [28]. Importantly the two-roundtrip periodicity of the nonlinear motion leads to self-symmetrization that eliminates all asymmetries, leading to the components $E_\pm$ experiencing identical detuning and driving terms. This complete self-symmetrization remains robust even in the presence of both an imperfect π-phase shift [referred to as δ_π in Fig. 1(b)] and an imperfectly aligned driving polarization [17].

Figure 1(c) displays predicted steady-state intensity values of the $E_\pm$ components obtained from solely even or odd roundtrips, with parameters similar to our experiments. Here, the intensities are plotted versus the detuning between the frequency of the driving laser and a closest cavity resonance of mode E_1, normalized to half the resonance linewidth. At low detunings, the two polarization projections $E_\pm$ are exactly equal. Symmetry breaking occurs above a certain threshold, manifesting itself through the parting of the two intensities of the polarization modes. Once the detuning is sufficiently large, the symmetry-broken 'bubble' closes, and the intensity levels become equal again. Thanks to the self-symmetrization that occurs as a result of the π-phase defect, repeated scanning of a control parameter [e.g. cavity detuning as in Fig. 1(c)] leads to random selection between the two possible states in the $E_\pm$ basis in a way that is immune to asymmetries [10]. By measuring the intensity of one of the circular polarization projections $E_\pm$ and assigning a value of '1' to high intensity measurements and '0' to low intensity measurements, the mechanism can be used for robust generation of random bit sequences. Our all-optical RNG is founded on this principle.

Figure 2 illustrates the key components of our experimental setup. The cavity consists of 57 m of MetroCor single-mode fibre with a Kerr nonlinearity coefficient of $\gamma = 2.5\ \text{W}^{-1}\text{km}^{-1}$. The fiber exhibits normal group-velocity dispersion at the driving wavelength of 1552 nm, thus ensuring suppression of modulation instabilities. A polarization controller [PC1 in Fig. 1] is used to align the driving field along one of the principal polarization modes of the cavity. A second, intra-cavity polarization controller [PC2 in Fig. 2] is used to introduce a phase defect of π between the two principal polarization modes. A 95:5 coupler injects the input field into the cavity, and a 99:1 coupler extracts a part of the circulating field, yielding a total cavity finesse of 40. After the 99:1 coupler, we project the output field onto the $E_\pm$ basis using a polarization controller [PC3 in Fig. 2], before separating these two components using a polarization beam splitter (PBS) and measuring their intensity profiles by means of fast-photodetectors connected to a real-time oscilloscope.

The resonator is coherently-driven with a train of 2-ps-

long pulses derived from an electro-optic (EO) comb generator seeded with a narrow-linewidth continuous-wave (CW) laser at 1552 nm. The EO comb generator consist of a cascade of two phase and one amplitude modulator followed by a nonlinear pulse compression stage. The repetition rate of the EO comb is derived from an external RF clock synthesizer that is carefully adjusted to be a large integer multiple of the cavity free-spectral range (FSR) of 3.655 MHz. We use an additional electro-optic modulator driven by a pulse-pattern generator to control the repetition rate of the driving pulses as desired before they are injected into the resonator. The experiments that will follow used an injection repetition rate of 1.17 GHz, such that there are 320 pulses circulating in the cavity simultaneously, separated in time by 0.8 ns. Each of the pulses undergoes SSB independently, thus allowing for an increased rate of random number generation via time-multiplexing. In this context, we emphasize that even though the pulses are only 2-ps-long, they undergo SSB in a manner that is qualitatively similar to the SSB of the CW states visualised in Fig. 1(c).

The experiments that will follow used an injection repetition rate of 1.17 GHz, such that there are

In order to repeatedly scan the cavity detuning back and forth across the SSB bifurcation point, we first actively stabilize the detuning within the symmetry-breaking regime using the technique described in [29]. We subsequently use an acousto-optic modulator (AOM) to sinusoidally modulate the frequency of the main pump beam, resulting in periodic scanning across the SSB bifurcation point at a frequency of 10 kHz. This causes the system to periodically switch between symmetric and symmetry-broken regimes, with each pulse randomly selecting one of the two possible solution states beyond the SSB bifurcation point. By detecting the intracavity pulse intensities following the bifurcation, a sequence of random bits is obtained. The 10 kHz modulation frequency and 320 pulses per roundtrip result in a generation of random bits at a speed of 3.2 Mbit/s.

Although based upon the same principle as the setup used in [17], our current configuration has been optimised to enable random number generation at significantly higher data rates than in [17]. Thanks to their much shorter duration, the electro-optically generated 2 ps pulses can be more closely spaced and more efficiently amplified, thus allowing for more efficient time-multiplexing and correspondingly higher data rates than the original experiment, which relied on 1.1-ns-long quasi-cw pulses. Our cavity is also five times longer than the one used in [17], which further increases the number of pulses that can simultaneously circulate in the resonator.

Figure 3 shows illustrative experimental results that demonstrate the generation of random bit sequences in our system. In these experiments, we recorded a long time series in real time on an oscilloscope as the detuning was scanned across the SSB bifurcation point. We then sliced the time series into individual segments spanning a single roundtrip: the pseudocolour plot in Fig. 3(a) corresponds to a horizontal concatenation of these segments to reveal the spatio-temporal evolution of the intracavity intensity of the circular polarization states (with only four bits shown for clarity). The SSB dynamics are hidden by the period-2 alternation that occurs in the measurement of a single circular polarization state, and is thus not directly visible in Fig. 3(a); however, when we only consider every second roundtrip, we clearly see the emergence of two states with differing intensity [Fig. 3(b,d)]. Figure 3(c,e) shows SSB results from a second experimental realization, demonstrating the generation of a new, independent bit sequence.

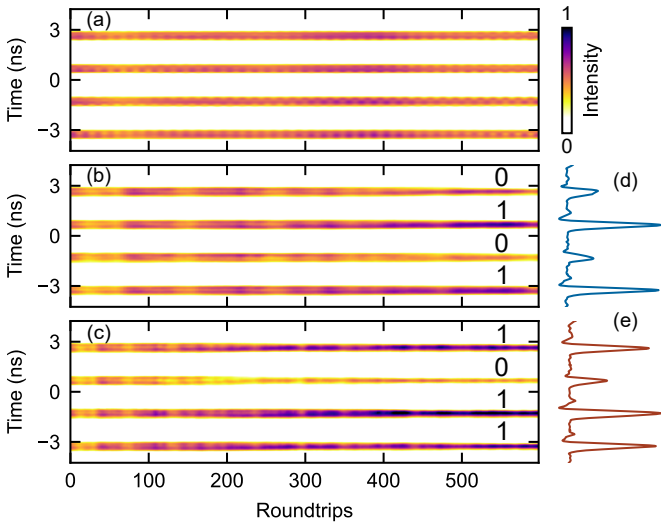

Fig. 3. **(a)** Evolution of the intracavity temporal intensity profiles corresponding to *one* of the circular polarization states as the detuning is scanned over consecutive roundtrips. **(b)-(c)** Evolution of the intracavity temporal intensity profiles when considering every second roundtrip for two independent realizations of the RNG system. **(d)-(e)** Temporal intensity profiles at the final roundtrip for each realization.

To confirm the true randomness of the bit sequences generated by our scheme, we implemented three separate statistical tests. First, Fig. 4(a) shows results from the National Institute of Standards and Technology (NIST) Statistical test Suite for RNGs (NIST STS-2.1.2) [20] applied to a sample of 32 million bits. Each test is applied to 100 samples from the entire 32 million-bit sequence, and each of these trials returns a p-value — the probability of this result occurring under the null hypothesis of a truly random source. NIST recommends that the minimum proportion of trials with a p-value greater than 0.01 be at least 96% for any given test. The bit sequences generated from our system pass this condition for every test [Fig. 4(b)].

As a second test, we consider the entropy generated by the system. In the ideal situation, each bit has an entropy of 1, which implies that each generated bit simulates a perfectly random coin toss. Following the method outlined by Steinle et al. [19], we show in Fig. 4(c) the conditional entropy — a measure of the system's memory — computed for our sequence of 32 millions bits. Each data point shows the distance from perfect entropy for a single trial of sample size N, while the top and orange lines show bounds for one bit-flip from perfect entropy and one standard deviation from the expected conditional Shannon entropy, respectively. We calculate the entropy considering both the conditional probability of individual bits **1** and **0**, as well as the probabilities for the tuples **11, 10, 01, 00** (e.g. the probability of observing the tuple **11** given that it follows the tuple **00**). We find that both the mean (magenta line), and the vast majority of the individual trials exhibit entropy values within one standard deviation of what is expected for an unbiased system, which gives us confidence that each bit generated can be used as a random bit without further processing [19].

Finally, Fig. 4(d) shows the results of the Dieharder tests applied to our bit stream [21]. Each Dieharder test consists of 100-1000 trials applied to subsets of our input data. A Kolmogorov-Smirnov (KS) test is then applied to the p-values obtained by each of these tests to determine the probability of observing the

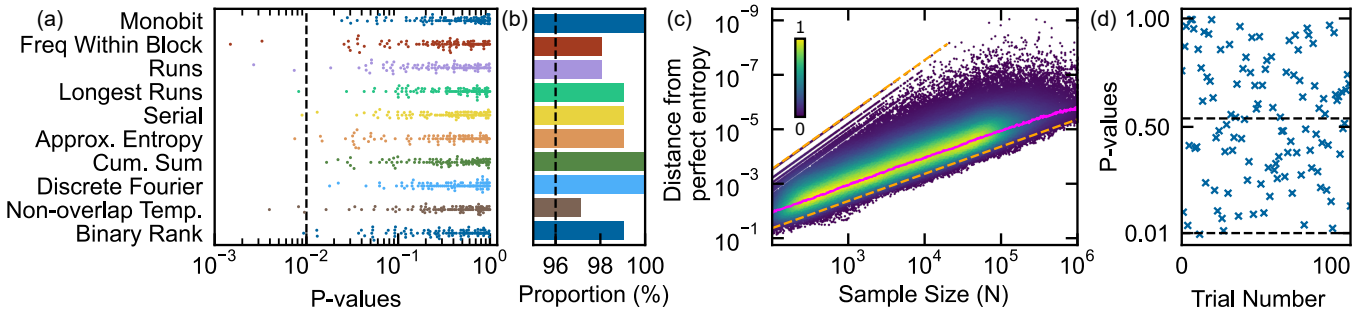

Fig. 4. Test results for randomness. **(a)** P-values generated by applying the NIST statistical tests to 100 samples of a 32 million bit sequence. **(b)** proportion of trials that pass the tests with the significance level of 0.01, which should be greater than 96%. **(c)** Shannon entropy in the generated bit-stream. The top and bottom orange lines show one bit-flip away from perfect entropy, and one standard deviation from the expected entropy generated by a random sequence, respectively. The individual points on the graph indicate the distance from perfect entropy for a given sample size, and the color gradient highlights the density of overlapping points. Finally, the magenta line shows the average of all individual trials. **(d)** P-values generated by application of the full suite of Dieharder Statistical tests. Horizontal dashed lines show the average of the test results (0.53) and the failure threshold (0.01).

distribution of p-values in the random sampling of a uniform distribution. These KS p-values are plotted in Figure 4(d). The random distribution of p-values centred at 0.53 and only a single failure occurring at the 0.01 significance level over all 113 tests shows that we have no evidence against the null hypothesis that our RNG is a truly random source.

To conclude, we have experimentally demonstrated an all-optical random number generator based on polarization symmetry breaking in a coherently-driven passive Kerr resonator. We achieved bit generation rates in excess of 3 MHz without any post-processing, which we believe can be further increased by optimising the cavity design and the modulation used to scan across the SSB bifurcation. Preliminary analysis suggests that operation in a microresonator platform has the potential to enable bit generation rates in the GHz range. We verified the randomness of the generated bit sequences using several statistical tests. In addition to representing a new avenue for physical random number generation, our work suggests that polarization symmetry breaking could be used to realise novel optical Ising or Potts machines.

Funding. Dodd-Walls Centre for Photonic and Quantum Technologies. Marsden Funding (18-UOA-310) from the Royal Society Te Apārangi. CNRS (IRP Wall-IN project), FEDER-FSE Bourgogne 2014/2020 programs, Conseil Régional de Bourgogne Franche-Comté.

Acknowledgements.

Disclosures. The authors declare no conflicts of interest.

Data Availability. The underlying data in this paper is not publicly available at this time, however it may be obtained from the authors upon reasonable request.

REFERENCES

1. P. Del'Haye, A. Schliesser, O. Arcizet, T. Wilken, R. Holzwarth, and T. J. Kippenberg, Nature **450**, 1214 (2007).
2. T. J. Kippenberg, R. Holzwarth, and S. A. Diddams, science **332**, 555 (2011).
3. B. Stern, X. Ji, Y. Okawachi, A. L. Gaeta, and M. Lipson, Nature **562**, 401 (2018).
4. S. Coen and M. Erkintalo, "Temporal Cavity Solitons in Kerr Media," in *Nonlinear Optical Cavity Dynamics,* P. Grelu, ed. (Wiley-VCH Verlag GmbH & Co. KGaA, Weinheim, Germany, 2015), pp. 11–40.
5. B. Garbin, J. Fatome, G.-L. Oppo, M. Erkintalo, S. G. Murdoch, and S. Coen, Phys. Rev. Lett. **126**, 023904 (2021).
6. S.-P. Yu, D. C. Cole, H. Jung, G. T. Moille, K. Srinivasan, and S. B. Papp, Nat. Photonics **15**, 461 (2021).
7. L. Del Bino, J. M. Silver, S. L. Stebbings, and P. Del'Haye, Sci. Reports **7**, 1 (2017).
8. Q.-T. Cao, H. Wang, C.-H. Dong, H. Jing, R.-S. Liu, X. Chen, L. Ge, Q. Gong, and Y.-F. Xiao, Phys. Rev. Lett. **118**, 033901 (2017).
9. M. T. Woodley, J. M. Silver, L. Hill, F. Copie, L. Del Bino, S. Zhang, G.-L. Oppo, and P. Del'Haye, Phys. Rev. A **98**, 053863 (2018).
10. B. Garbin, J. Fatome, G.-L. Oppo, M. Erkintalo, S. G. Murdoch, and S. Coen, Phys. Rev. Res. **2**, 023244 (2020).
11. G. Xu, A. U. Nielsen, B. Garbin, L. Hill, G.-L. Oppo, J. Fatome, S. G. Murdoch, S. Coen, and M. Erkintalo, Nat Commun **12**, 4023 (2021).
12. B Garbin, A Giraldo, K J H Peters, N G R Broderick, A Spakman, F Raineri, A Levenson, S R K Rodriguez, B Krauskopf, and A M Yacomotti, Phys. Rev. Lett. **128**, 053901 (2022).
13. M. Haelterman, S. Trillo, and S. Wabnitz, J. Opt. Soc. Am. B **11**, 446 (1994).
14. T. Stojanovski and L. Kocarev, IEEE Trans. on Circuits Syst. I: Fundam. Theory Appl. **48**, 281 (2001).
15. X. Yuan, Z. Cao, and X. Ma, Phys. Rev. A **91**, 032111 (2015).
16. H. Crauel and F. Flandoli, J. Dyn. Differ. Equations **10**, 259 (1998).
17. S. Coen, B. Garbin, G. Xu, L. Quinn, N. Goldman, G.-L. Oppo, M. Erkintalo, S. G. Murdoch, and J. Fatome, arXiv preprint arXiv:2303.16197 (2023).
18. G. Steinmeyer, D. Jaspert, and F. Mitschke, Opt. Commun. **104**, 379 (1994).
19. T. Steinle, J. N. Greiner, J. Wrachtrup, H. Giessen, and I. Gerhardt, Phys. Rev. X **7**, 041050 (2017).
20. A. Rukhin, J. Soto, J. Nechvatal, M. Smid, and E. Barker, "A statistical test suite for random and pseudorandom number generators for cryptographic applications," Tech. rep., National Institute of Standards and Technology (2001).
21. R. G. Brown, D. Eddelbuettel, and D. Bauer, Duke Univ. Phys. Dep. pp. 27708–0305 (2018).
22. A. Marandi, N. C. Leindecker, K. L. Vodopyanov, and R. L. Byer, Opt. Express **20**, 19322 (2012).
23. Y. Okawachi, M. Yu, K. Luke, D. O. Carvalho, M. Lipson, and A. L. Gaeta, Opt. Lett. **41**, 4194 (2016).
24. Z. Wang, A. Marandi, K. Wen, R. L. Byer, and Y. Yamamoto, Phys. Rev. A **88**, 063853 (2013).
25. T. Inagaki, Y. Haribara, K. Igarashi, T. Sonobe, S. Tamate, T. Honjo, A. Marandi, P. L. McMahon, T. Umeki, and K. Enbutsu, Science **354**, 603 (2016).
26. P. L. McMahon, A. Marandi, Y. Haribara, R. Hamerly, C. Langrock, S. Tamate, T. Inagaki, H. Takesue, S. Utsunomiya, K. Aihara, R. L. Byer, M. M. Fejer, H. Mabuchi, and Y. Yamamoto, Science **354**, 614 (2016).
27. M. Honari-Latifpour and M.-A. Miri, Nanophotonics **9**, 4199 (2020).
28. L. A. Lugiato and R. Lefever, Phys. review letters **58**, 2209 (1987).
29. A. U. Nielsen, B. Garbin, S. Coen, S. G. Murdoch, and M. Erkintalo, APL Photonics **3**, 120804 (2018).