

Microresonator-Based Quantum Random Number Generator

Yoshitomo Okawachi¹, Mengjie Yu^{1,2}, Kevin Luke², Daniel O. Carvalho^{2,3},
Michal Lipson⁴, and Alexander L. Gaeta¹

¹Department of Applied Physics and Applied Mathematics, Columbia University, New York, NY 10027

²School of Electrical and Computer Engineering, Cornell University, Ithaca, NY 14853

³current address: São Paulo State University (UNESP), São João da Boa Vista, Brazil

⁴Department of Electrical Engineering, Columbia University, New York, NY 10027

Author e-mail address: y.okawachi@columbia.edu

Abstract: We demonstrate quantum random number generation at 2 Mbps using binary phase state generation via degenerate optical parametric oscillation in a silicon-nitride microresonator. Such a system can potentially scale to rates > 1 Gbs.

OCIS codes: (190.4380) Four-wave mixing; (190.4970) Parametric oscillators and amplifiers; (190.4390) Integrated optics

Random number generators (RNG's) are a critical component for applications including cryptography, Monte Carlo simulations, statistical sampling, and quantitative finance [1]. To meet the requirements of these applications, there has been significant work done on the development of RNG's that are low cost and operate with high generation rates while maintaining a high degree of randomness. While many algorithms exist in computer programming for random number generation, these generate pseudo-random numbers are not truly indeterministic [2]. Alternatively, RNG's based on quantum mechanical systems have been studied in which the phenomenon is intrinsically random [2,3]. However, many of these systems require extensive modeling of the quantum process for significant post-processing or characterization of the source and readout device to guarantee that the output is truly random, which limits the generation rate. Recently, there has been a demonstration of an quantum RNG using a $\chi^{(2)}$ -based degenerate optical parametric oscillator (OPO) [4]. Here, the system utilizes the binary state generation that is enabled by the frequency degenerate operation of the OPO, where the generated signal field phase-locks to the pump field with two possible states that are offset by π . Since oscillation is initiated from quantum noise, the system is intrinsically unbiased and only requires the detection of strong, classical signals with no post-processing, which greatly reduces the complexity and required computational overhead. Furthermore, this binary phase state generation using the degenerate OPO has been shown to be analogous to a binary spin system, and this spin-like behavior is crucial for realizing a novel form of coherent computing by simulating the classical Ising model [5,6]. A network of coupled OPO's offers the potential for solving nondeterministic polynomial time (NP)-hard computation problems.

In this paper, we demonstrate an all-optical quantum RNG based on bi-phase state generation using a dual-pumped degenerate OPO in a silicon nitride (Si_3N_4) microresonator. Recent work has shown that a $\chi^{(3)}$ -based OPO offers dynamics that mirrors the $\chi^{(2)}$ system [7-9]. The parametric oscillation in this case utilizes parametric four-wave mixing (FWM) interactions, where two frequency non-degenerate pumps are annihilated to generate a frequency-degenerate signal/idler pair. The FWM process is dictated by the phase matching conditions $\Delta\phi = \phi_1 + \phi_2 - 2\phi_3$, where ϕ_1 and ϕ_2 are the phase of the two pumps, and ϕ_3 is the phase of the generated signal/idler pair. From this equation, the same phase matching conditions exist for a π phase shift in the generated field, thus allowing for a bi-phase state that is offset by π . The $\chi^{(3)}$ nonlinear process allows for use with silicon-based photonics technology, and Si_3N_4 is a particularly favorable platform for operation in the near-infrared regime, since it is CMOS-process compatible, has low losses and a high nonlinearity, and allows for dispersion engineering [10], which is critical for efficient FWM processes and enabling bi-phase state operation [7]. We achieve a generation rate of 2 Mbps by amplitude modulation of one of the two pump lasers. We verify the generation of the bi-phase state using an asymmetric Mach-Zehnder interferometer to measure the relative phase between adjacent bits in the generated pulse train. In addition, we analyze our sample bits using the National Institute of Standards and Technology (NIST) Statistical Test Suite to verify the randomness of our generated output.

To realize degenerate oscillation, we require a frequency non-degenerate dual-pump configuration and operation in the normal group-velocity dispersion (GVD) regime. In order to achieve maximum parametric gain at the frequency degeneracy point, the two pumps are offset by frequency $\pm\delta$ from the degeneracy point such that the dispersion length $L_D = 1/\delta^2|\beta_2|$ is larger than the nonlinear length $L_{NL} = 1/2\gamma P$, where β_2 is the GVD parameter, γ is the nonlinear parameter, and P is the power for each pump [7]. In our experiment (Fig. 1), the pumps are generated by amplifying two tunable single-frequency pump lasers. The wavelengths of the two pumps are set to 1557.8 nm and 1542.2 nm,

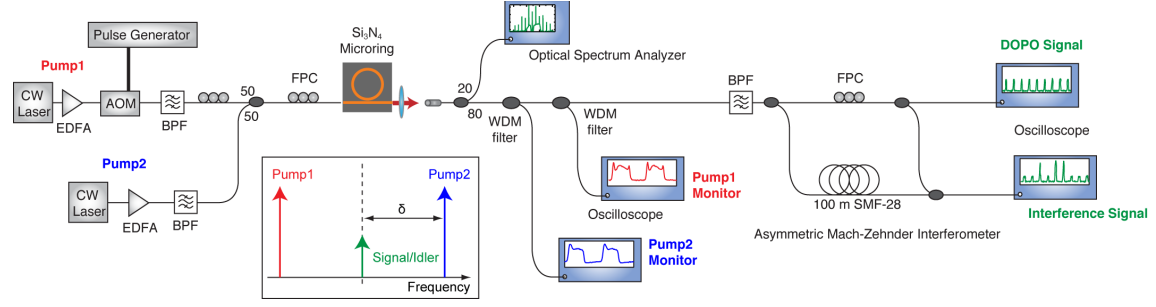


Fig. 1. Experimental setup for RNG using degenerate OPO. The power of pump1 is modulated using an acousto-optic modulator (AOM). Both pumps are modulated using a photodiode and an oscilloscope to ensure that they are tune to the microresonator resonance. The generated bi-phased state is characterized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

which correspond to 4 FSR's from the frequency degeneracy point. We modulate the amplitude of the pump at 1557.8 nm using an acousto-optic modulator (AOM) driven with 250-ns pulses at a 2 MHz repetition rate. The duration, amplitude, and DC offset of the modulation is chosen to take into account thermal effects in the resonator to optimize OPO generation. The input polarization of the two pumps is set to the quasi-TM mode. The Si_3N_4 microresonator has an effective cross section of 690×1300 nm, which allows for normal GVD for the TM polarization mode. To achieve parametric oscillation, we tune each pump into a microresonator cavity resonance, taking into account the thermal frequency shift that occurs due to pump power build-up. The combined pump power in the coupling waveguide is 128 mW. Figure 2(a) shows the optical spectrum of the generated OPO, where the degenerate signal is at 1551.5 nm. To verify the bi-phase state generation, we use a bandpass filter to transmit only the degenerate OPO signal and send it to an asymmetric Mach-Zehnder interferometer, which has an extra 100-m length of SMF-28 fiber in one arm to allow for characterization of the relative phase between adjacent bits. Constructive interference and destructive interference

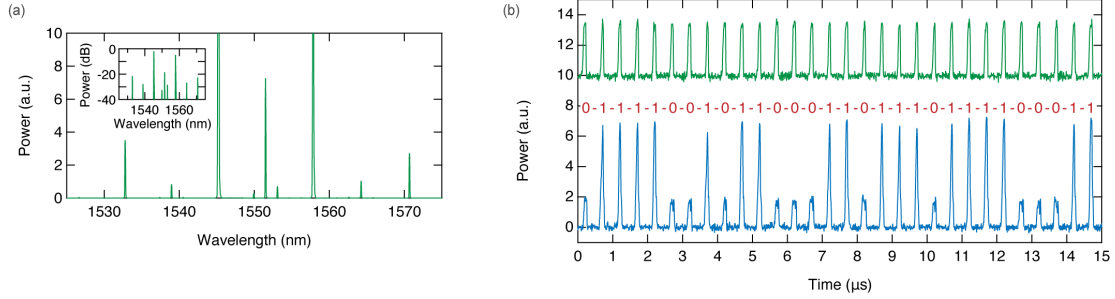


Fig. 2. (a) Optical spectrum for degenerate $\chi^{(3)}$ OPO in Si_3N_4 microresonator. (b) Temporal measurement of degenerate OPO RNG. Plot shows the OPO output (green) and the asymmetric Mach-Zehnder interferometer output (blue).

corresponds to a relative phase of 0 and π , respectively. In addition, we insert a 50/50 splitter into one arm of the interferometer to simultaneously measure the amplitude of the degenerate OPO signal.

Figure 2(b) shows the temporal measurement of the degenerate OPO output (green) and the interferometer output (blue). The maximum and minimum amplitudes in the interferometer output correspond to constructive and destructive 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. The verification of bi-state generation is critical for random number generation and a significant step towards the realization of a chip-based photonic Ising machine using coupled OPO's. Finally, to test the randomness of our output, we use the NIST Statistical Test Suite (STS-2.1.2), which consists of a series of statistical hypothetical tests designed to detect non-randomness and assess proportion and uniformity [11]. Our sample consists of 217,000 bits which are divided into 100 samples of equal length. The results are shown in Fig. 3. The Final Analysis Report indicates that the minimum pass rate for each statistical test is 96%, indicating that our sample passes each of the NIST tests.

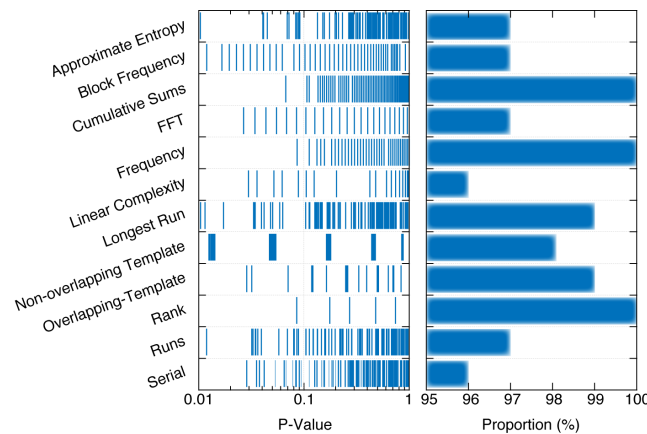


Fig. 3. Test results for randomness using NIST Statistical Test Suite. Sample consists of 100 sets of 2170 bits. The p-value indicates the probability that a perfect RNG outputs a sequence that is less random than the test sequence. The proportion indicates the percentage of sequences that pass the test with a significance level >0.01 , which indicates the upper bound for the probability of incorrectly rejecting the null hypothesis.

In conclusions, we demonstrate a quantum RNG in a silicon microresonator. Our generation rate is currently 2 Mbps and is largely dependent on the pump power, cavity lifetime of the microresonator [4], and thermal effects in Si_3N_4 . Since our OPO operates above threshold, our scheme involves detection of classical signals which significantly simplifies the complexity of the system. Our generation rate can be further increased beyond 1 Gbps while maintaining a compact footprint by using a system of time-multiplexed OPO's. Our scheme offers potential for a compact chip-scale RNG with applications such as cryptography, computer programming, and Monte-Carlo simulations. In addition, we believe our scheme offers a significant step towards a chip-based coherent Ising machine using a network of coupled-OPO's.

References

- [1] A. Stefaov, N. Gisin, O. Guinnard, L. Guinnard, and H. Zbinden, "Optical quantum random number generator," *J. Mod. Opt.* **37**, 595 (2000).
- [2] X. Ma, Y. Yuan, Z. Cao, B. Qi, and Z. Zhang, "Quantum random number generation," *NPJ Quantum Inf.* **2**, 16021 (2016).
- [3] M. Herrero-Collantes and J. C. Garcia-Escartin, "Quantum random number generators," *Rev. Mod. Phys.* **89**, 015004 (2017).
- [4] A. Marandi, N. C. Leindecker, K. L. Vodopyanov, and R. L. Byer, "All-optical quantum random bit generation from intrinsically binary phase of parametric oscillators," *Opt. Express* **20**, 19322 (2012).
- [5] T. Inagaki, *et al.*, "A coherent Ising machine for 2000-node optimization problems," *Science* **354**, 603 (2016).
- [6] P. L. McMahon, *et al.*, "A fully programmable 100-spin coherent Ising machine with all-to-all connections," *Science* **354**, 614 (2016).
- [7] Y. Okawachi, *et al.*, "Dual-pumped degenerate Kerr oscillator in a silicon nitride microresonator," *Opt. Lett.* **40**, 5267 (2015).
- [8] T. Inagaki, K. Inaba, R. Hamerly, K. Inoue, Y. Yamamoto, and H. Takesue, "Large-scale Ising spin network based on degenerate optical parametric oscillators," *Nat. Photonics* **10**, 415 (2016).
- [9] H. Takesue and T. Inagaki, "10 GHz clock time-multiplexed degenerate optical parametric oscillators for a photonic Ising spin network," *Opt. Lett.* **41**, 4273 (2016).
- [10] D. J. Moss, R. Morandotti, A. L. Gaeta, and M. Lipson, "New CMOS-compatible platforms based on silicon nitride and Hydex for nonlinear optics," *Nat. Photonics* **7**, 597 (2013).
- [11] A. Rukhin, *et al.*, "A statistical test suite for random and pseudorandom number generators for cryptographic applications," NIST special publication 800-22, Rev. 1-a, NIST, Gaithersburg, Maryland, USA, (2010).