Fast physical random number generator using amplified spontaneous emission

Caitlin R. S. Williams,[1,2,*] **Julia C. Salevan,**[1] **Xiaowen Li,**[2,3] **Rajarshi Roy,**[1,2,4] **and Thomas E. Murphy**[2,5]

[1]*Dept. of Physics, University of Maryland, College Park, Maryland 20742, USA*
[2]*Institute for Research in Electronics and Applied Physics, University of Maryland, College Park, Maryland 20742, USA*
[3]*Dept. of Physics, Beijing Normal University, Beijing 100875, China*
[4]*Institute for Physical Science and Technology, University of Maryland, College Park, Maryland 20742, USA*
[5]*Dept. of Electrical and Computer Engineering, University of Maryland, College Park, Maryland 20742, USA*

[*]*willcrs@umd.edu*

Abstract: We report a 12.5 Gb/s physical random number generator (RNG) that uses high-speed threshold detection of the spectrally-sliced incoherent light produced by a fiber amplifier. The system generates a large-amplitude, easily measured, fluctuating signal with bandwidth that is constrained only by the optical filter and electrical detector used. The underlying physical process (spontaneous emission) is inherently quantum mechanical in origin, and therefore cannot be described deterministically. Unlike competing optical RNG approaches that require photon counting electronics, chaotic laser cavities, or state-of-the-art analog-to-digital converters, the system employs only commonly available telecommunications-grade fiber optic components and can be scaled to higher speeds or multiplexed into parallel channels. The quality of the resulting random bitstream is verified using industry-standard statistical tests.

OCIS codes: (030.6600) Statistical optics; (060.0060) Fiber optics and optical communications; (230.2285) Fiber devices and optical amplifiers; (060.2320) Fiber optics amplifiers and oscillators; (270.2500) Fluctuations, relaxations, and noise.

References and links

1. A. M. Ferrenberg, D. P. Landau, and Y. J. Wong, "Monte Carlo simulations: hidden errors from 'good' random number generators," Phys. Rev. Lett. **69**, 3382–3384 (1992).
2. M. Isida and H. Ikeda, "Random number generator," Ann. Inst. Stat. Math. **8**, 119–126 (1956).
3. J. Walker, "HotBits: Genuine random numbers, generated by radioactive decay," Online: http://www.fourmilab.ch/hotbits/.
4. W. T. Holman, J. A. Connelly, and A. B. Dowlatabadi, "An integrated analog/digital random noise source," IEEE Trans. Circuits Syst., I: Fundam. Theory Appl. **44**, 521–528 (1997).
5. P. Xu, Y. Wong, T. Horiuchi, and P. Abshire, "Compact floating-gate true random number generator," Electron. Lett. **42**, 1346 –1347 (2006).
6. C. Petrie and J. Connelly, "A noise-based IC random number generator for applications in cryptography," IEEE Trans. Circuits Syst., I: Fundam. Theory Appl. **47**, 615–621 (2000).
7. B. Jun and P. Kocher, "The Intel Random Number Generator," Cryptography Research Inc., white paper prepared for Inter Corp. (1999).
8. M. Bucci, L. Germani, R. Luzzi, A. Trifiletti, and M. Varanonuovo, "A high-speed oscillator-based truly random number source for cryptographic applications on a smart card IC," IEEE Trans. Comput. **52**, 403–409 (2003).

#134856 - $15.00 USD Received 9 Sep 2010; revised 19 Oct 2010; accepted 20 Oct 2010; published 26 Oct 2010

9. G. Bernstein and M. Lieberman, "Secure random number generation using chaotic circuits," IEEE Trans. Circuits Syst. **37**, 1157–1164 (1990).
10. T. Stojanovski and L. Kocarev, "Chaos-based random number generators – Part I: analysis," IEEE Trans. Circuits Syst., I: Fundam. Theory Appl. **48**, 281–288 (2001).
11. T. Stojanovski, J. Pihl, and L. Kocarev, "Chaos-based random number generators – Part II: practical realization," IEEE Trans. Circuits Syst., I: Fundam. Theory Appl. **48**, 382–385 (2001).
12. M. Haahr, "Random.org: True Random Number Service," Online: http://www.random.org/.
13. T. Jennewein, U. Achleitner, G. Weihs, H. Weinfurter, and A. Zeilinger, "A fast and compact quantum random number generator," Rev. Sci. Instrum. **71**, 1675–1680 (2000).
14. J. F. Dynes, Z. L. Yuan, A. W. Sharpe, and A. J. Shields, "A high speed, postprocessing free, quantum random number generator," Appl. Phys. Lett. **93**, 031109 (2008).
15. C. Gabriel, C. Wittmann, D. Sych, R. Dong, W. Mauerer, U. L. Andersen, C. Marquardt, and G. Leuchs, "A generator for unique quantum random numbers based on vacuum states," Nature Photon. **4**, 711–715 (2010).
16. L. C. Noll and S. Cooper, "What is LavaRnd?" Online: http://www.lavarnd.org/.
17. B. Qi, Y.-M. Chi, H.-K. Lo, and L. Qian, "High-speed quantum random number generation by measuring phase noise of a single-mode laser," Opt. Lett. **35**, 312–314 (2010).
18. H. Guo, W. Tang, Y. Liu, and W. Wei, "Truly random number generation based on measurement of phase noise of a laser," Phys. Rev. E **81**, 051137 (2010).
19. A. Uchida, K. Amano, M. Inoue, K. Hirano, S. Naito, H. Someya, I. Oowada, T. Kurashige, M. Shiki, S. Yoshimori, K. Yoshimura, and P. Davis, "Fast physical random bit generation with chaotic semiconductor lasers," Nature Photon. **2**, 728–732 (2008).
20. I. Reidler, Y. Aviad, M. Rosenbluh, and I. Kanter, "Ultrahigh-speed random number generation based on a chaotic semiconductor laser," Phys. Rev. Lett. **103**, 024102 (2009).
21. A. Argyris, S. Deligiannidis, E. Pikasis, A. Bogris, and D. Syvridis, "Implementation of 140 Gb/s true random bit generator based on a chaotic photonic integrated circuit," Opt. Express **18**, 18763–18768 (2010). http://www.opticsexpress.org/abstract.cfm?URI=oe-18-18-18763.
22. I. Kanter, Y. Aviad, I. Reidler, E. Cohen, and M. Rosenbluh, "An optical ultrafast random bit generator," Nature Photon. **4**, 58–61 (2010).
23. K. Hirano, T. Yamazaki, S. Morikatsu, H. Okumura, H. Aida, A. Uchida, S. Yoshimori, K. Yoshimura, T. Harayama, and P. Davis, "Fast random bit generation with bandwidth-enhanced chaos in semiconductor lasers," Opt. Express **18**, 5512–5524 (2010). http://www.opticsexpress.org/abstract.cfm?URI=oe-18-6-5512.
24. N. A. Olsson, "Lightwave systems with optical amplifiers," J. Lightwave Technol. **7**, 1071–1082 (1989).
25. R. C. Steele, G. R. Walker, and N. G. Walker, "Sensitivity of optically preamplified receivers with optical filtering," IEEE Photon. Technol. Lett. **3**, 545–547 (1991).
26. M. S. Leeson, "Performance analysis of direct detection spectrally sliced receivers using Fabry-Perot filters," J. Lightwave Technol. **18**, 13–25 (2000).
27. J. W. Goodman, *Statistical Optics* (Wiley, 1985). p. 246.
28. P. A. Humblet and M. Azizoğlu, "On the bit error rate of lightwave systems with optical amplifiers," J. Lightwave Technol. **9**, 1576–1582 (1991).
29. A. J. Keating and D. D. Sampson, "Reduction of excess intensity noise in spectrum-sliced incoherent light for WDM applications," J. Lightwave Technol. **15**, 53–61 (1997).
30. J.-S. Lee, "Signal-to-noise ratio of spectrum-sliced incoherent light sources including optical modulation effects," J. Lightwave Technol. **14**, 2197–2201 (1996).
31. D. Knuth, *The Art of Computer Programming, Volume 2: Seminumerical Algorithms (3rd ed.)* (Addison-Wesley, 1996). pp. 64–65.
32. 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 Special Publication 800-22, Revision 1a)*, National Institute of Standards and Technology (2010).
33. G. Marsaglia, "DIEHARD: A battery of tests of randomness," Online: http://www.stat.fsu.edu/pub/diehard/ (1996).
34. S. Pironio, A. Acín, S. Massar, A. B. de la Giroday, D. N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T. A. Manning, and C. Monroe, "Random numbers certified by Bell's theorem," Nature **464**, 1021–1024 (2010).
35. R. H. Walden, "Analog-to-digital converter survey and analysis," IEEE J. Sel. Areas Commun. **17**, 539–550 (1999).

#134856 - $15.00 USD Received 9 Sep 2010; revised 19 Oct 2010; accepted 20 Oct 2010; published 26 Oct 2010

1. Introduction

Random number generators are important for a variety of applications, including encryption, secure key generation, gaming and Monte-Carlo calculations. Most of these applications employ pseudo-random number generators (PRNGs) – deterministic algorithms implemented on a computer or dedicated hardware that generate a seemingly unpredictable sequence of bits that are statistically indistinguishable from a truly random sequence. Although PRNGs are cost-effective and, in most cases, efficient, they suffer from the vulnerability that the future (and in some cases past) sequence can be deterministically computed if one discovers the seed or internal state of the algorithm. In weak PRNG algorithms, the internal state can be inferred by observing a sufficiently long history of the bit sequence. Even in Monte-Carlo simulations, where security is unimportant, pseudorandom number generators can yield erroneous results [1].

For these reasons, there is growing interest in physical random number generators that produce random bits from inherently random or chaotic physical processes. Examples of physical processes used for random number generation include radioactive decay [2, 3], electrical thermal noise [4, 5], timing jitter in electrical oscillators [6–8], chaotic electrical circuits [9–11], and atmospheric RF noise [12]. In general, these systems are slow in comparison to pseudorandom number algorithms. Increasingly, optical or optoelectronic systems are being explored for random number generation. Shot noise has been exploited to produce random bits at rates up to 4 Mb/s, using photon-counting detectors with weak lasers or LEDs [13, 14]. Optical homodyne detection of vacuum fluctuations has been used to produce random bits at a 6.5 Mb/s [15]. Dark noise collected from CCDs has been used as a seed for pseudorandom number generators [16]. Phase noise produced in a distributed feedback laser has been used to generate random bits at rates up to 500 Mb/s [17,18]. Recently, chaotic semiconductor lasers have been used to generate random bits at 1.7 Gb/s [19], or much faster when coupled with high-speed analog-to-digital conversion and digital post processing [20–23].

We report here a simple, scalable method of generating random bits using filtered amplified spontaneous emission (ASE) produced in a fiber amplifier. Spectrally-sliced ASE produces a fast, fluctuating signal that is much stronger than the background electronic noise, and can produce random bits at rates limited only by the bandwidths of the optical filter and electrical photoreceiver. Using only threshold detection and XOR decorrelation techniques, we achieve 12.5 Gb/s random number generation, and confirm the quality of the resulting random bit sequence using accepted statistical tests developed for cryptographic security. The system uses only standard fiber optic components found in conventional digital telecommunication systems, and could be easily multiplexed into parallel wavelength channels by using WDM filter technology to spectrally slice the ASE spectrum.

2. Theory

Amplified spontaneous emission is one of the most significant and ubiquitous noise sources in modern fiber optic telecommunication systems, and its statistical properties are well understood. In the present system, filtered amplified spontaneous emission noise is detected in a square-law photodetector, generating a noisy baseband electrical current that is referred to as "ASE-ASE beat noise." We summarize here the key relations that govern the power spectrum, signal-to-noise ratio, and probability distribution of ASE-ASE beat noise, as these terms ultimately govern the speed and performance of our random bit generator.

Fig. 1 is a block diagram that defines the key elements used to produce the noise signal from which we generate random numbers. The input optical noise signal $u(t)$ is taken to be white noise generated by amplified spontaneous emission with a power spectral density of S_0. We assume that the noise is polarized, both to simplify the analysis and also because that is how our experimental system is constructed. The noise passes through an optical bandpass filter

#134856 - $15.00 USD Received 9 Sep 2010; revised 19 Oct 2010; accepted 20 Oct 2010; published 26 Oct 2010

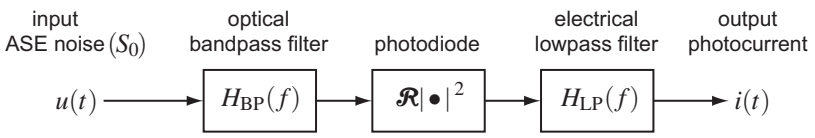

Fig. 1. Simplified block diagram of a spectrally-filtered ASE noise source. The input optical signal $u(t)$ is assumed to be white optical noise with spectral density S_0, which passes through a bandpass filter (H_{BP}), square-law photodetector with responsivity $\mathscr{R}$, and low-pass filter (H_{LP}) to produce an output photocurrent $i(t)$.

that has a (dimensionless) complex transfer function $H_{\mathrm{BP}}(f)$, so that the power spectral density of the emerging optical signal is $S_0|H_{\mathrm{BP}}(f)|^2$. The photodiode produces an electrical current proportional to the squared magnitude of the optical field, and the resulting photocurrent is passed through a low-pass filter with transfer function $H_{\mathrm{LP}}(f)$.

The photocurrent statistics depend on the characteristics of the bandpass and lowpass filters used. Therefore, in the equations that follow we provide both the general equation and also specific expressions for the case when both the bandpass and lowpass filters are Gaussian, i.e.,

$$|H_{\mathrm{BP}}(f)|^2 = \exp\left[-(4\ln 2)\frac{(f-f_0)^2}{B_{\mathrm{BP}}^2}\right], \qquad |H_{\mathrm{LP}}(f)|^2 = \exp\left[-(\ln 2)\frac{f^2}{B_{\mathrm{LP}}^2}\right], \tag{1}$$

where B_{BP} and B_{LP} represent the 3 dB bandwidths of the bandpass and lowpass filters, respectively.

The mean photocurrent generated by amplified spontaneous emission is proportional to the total integrated optical noise power,

$$\langle i\rangle = \mathscr{R}S_0H_{\mathrm{LP}}(0)\int \left|H_{\mathrm{BP}}(f)\right|^2 df \tag{2a}$$

$$= \mathscr{R}S_0B_{\mathrm{BP}}\sqrt{\frac{\pi}{4\ln 2}} \qquad \text{(Gaussian)}, \tag{2b}$$

where $\mathscr{R}$ denotes the responsivity of the photodiode, $H_{\mathrm{LP}}(0)$ is the DC gain of lowpass filter, and Eq. (2b) gives the specific result for the case of Gaussian filters. Because the responsivity $\mathscr{R}$ is typically measured at DC frequencies, one typically takes $H_{\mathrm{LP}}(0)=1$ with the assumption that any DC filter attenuation has been factored into $\mathscr{R}$.

The power spectral density of the photocurrent noise is given by [24, 25]

$$S_i(f) = \mathscr{R}^2S_0^2|H_{\mathrm{LP}}(f)|^2\int \left|H_{\mathrm{BP}}(f')H_{\mathrm{BP}}(f+f')\right|^2 df' \tag{3a}$$

$$= \mathscr{R}^2S_0^2B_{\mathrm{BP}}\sqrt{\frac{\pi}{8\ln 2}}\exp\left[-(\ln 2)\left(\frac{1}{B_{\mathrm{LP}}^2}+\frac{2}{B_{\mathrm{BP}}^2}\right)f^2\right] \qquad \text{(Gaussian)}, \tag{3b}$$

where, as before, Eq. (3a) gives the general expression and Eq. (3b) reflects the specific case when Gaussian filters are used. Note for the Gaussian filter case, the photocurrent noise spectrum will also be Gaussian, with a noise bandwidth of

$$B_{\mathrm{noise}} = \left(\frac{1}{B_{\mathrm{LP}}^2}+\frac{2}{B_{\mathrm{BP}}^2}\right)^{-1/2} \qquad \text{(Gaussian)}. \tag{4}$$

#134856 - $15.00 USD Received 9 Sep 2010; revised 19 Oct 2010; accepted 20 Oct 2010; published 26 Oct 2010

The photocurrent variance can be directly calculated by integrating the noise spectrum,

$$\sigma_i^2 = \int S_i(f)\,df = \mathscr{R}^2 S_0^2 \iint \left|H_{\rm LP}(f)H_{\rm BP}(f')H_{\rm BP}(f+f')\right|^2 df\,df' \tag{5a}$$

$$= \mathscr{R}^2 S_0^2 B_{\rm BP}^2 \left(\frac{\pi}{4\ln 2}\right)\left(1+\frac{B_{\rm BP}^2}{2B_{\rm LP}^2}\right)^{-1/2} \qquad \text{(Gaussian)}, \tag{5b}$$

where again, the second equation reflects the specific case of Gaussian bandpass and lowpass filters. Note that for simplicity, we have omitted the DC photocurrent contribution to $S_i(f)$, which would appear as a term proportional to $\langle i\rangle^2\,\delta(f)$. Thus, Eq. (3a) represents the power spectral density of the zero-mean process $i(t)-\langle i\rangle$.

The probability distribution of the photocurrent depends on the bandpass and lowpass filters used, and in general must be evaluated numerically [26]. However, in most practical cases of interest, the photocurrent probability distribution is well-approximated by a gamma distribution [27–29],

$$p_i(x) = x^{a-1}\frac{\exp(-x/b)}{b^a\Gamma(a)}, \qquad x>0, \tag{6}$$

where the dimensionless shape parameter a describes the signal to noise ratio [30],

$$a = \frac{\langle i\rangle^2}{\sigma_i^2} = \frac{H_{\rm LP}^2(0)\left(\int |H_{\rm BP}(f)|^2 df\right)^2}{\iint \left|H_{\rm LP}(f)H_{\rm BP}(f')H_{\rm BP}(f+f')\right|^2 df\,df'} \tag{7a}$$

$$= \left(1+\frac{B_{\rm BP}^2}{2B_{\rm LP}^2}\right)^{1/2} \qquad \text{(Gaussian)}. \tag{7b}$$

One interesting property of ASE-ASE beat noise, apparent from Eq. (7b), is that the signal-to-noise ratio (a) depends only on the shapes of the optical and electrical filters employed.

In a practical system, the mean photocurrent $\langle i\rangle$ cannot be too large, or else the photoreciever will saturate, producing only a DC output with no noise. This saturation will occur even if the output signal is AC-coupled. Therefore, in order to produce a strong electrical noise signal at the output without saturating the photoreceiver, one seeks to minimize the signal-to-noise ratio. From Eq. (7b), this can only be achieved by choosing bandpass and lowpass filters that have comparable bandwidths.

3. Experimental System

Fig. 2 depicts the experimental system used to generate random bits. As the source of noise, we use a fiber amplifier (Optical Air Data Systems) consisting of a 1 W, 915 nm semiconductor pump laser and an erbium/ytterbium co-doped fiber. When there is no input, the amplifier generates broadband, incoherent, unpolarized optical noise through amplified spontaneous emission (ASE). The optical spectrum of the output of the amplifier was measured with an optical spectrum analyzer and is shown in Fig. 3a. The optical bandwidth of the ASE is much larger than the electrical bandwidth of even a fast detector. If the ASE were directly detected, Eq. (7b) dictates that in order to produce a sufficient noise variance one would require an impractically large DC photocurrent. To overcome this limitation, the broadband optical noise from the amplifier is filtered by an optical bandpass filter, comprised of a fiber Bragg grating (FBG) (TeraXion) and optical circulator. Fig. 3b plots the spectrum of the bandpass filter assembly, measured using a tunable laser and power meter. The filter has an optical bandwidth of 14.5 GHz (0.1 nm) and center wavelength of λ_0 = 1552.5 nm. The resulting filtered noise signal is then amplified

#134856 - $15.00 USD Received 9 Sep 2010; revised 19 Oct 2010; accepted 20 Oct 2010; published 26 Oct 2010

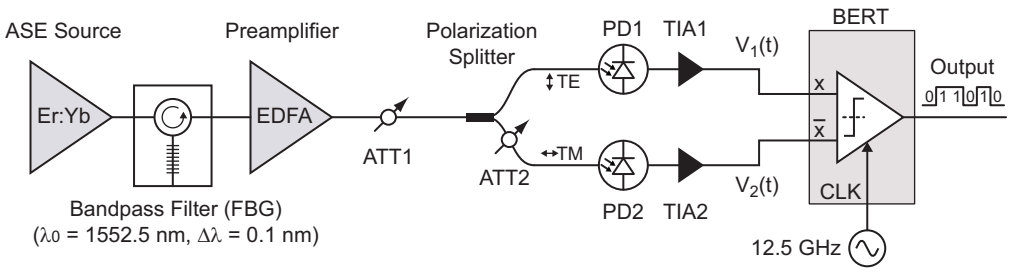

Fig. 2. System used to generate random bits at 12.5 Gb/s. Amplified spontaneous emission (ASE) is generated in an Er/Yb-doped fiber that is continuously pumped by a 1 W, fiber-coupled 915 nm semiconductor laser diode. The resulting broadband ASE spectrum is bandpass-filtered using a 14.5 GHz (0.1 nm) fiber Bragg grating and optical circulator. The filtered noise is amplified in a conventional Er-doped fiber amplifier (EDFA). A fiber polarization splitter is used to produce two independent, identically distributed optical noise signals that are separately detected in a pair of matched 11 GHz photoreceivers, each comprised of a photodiode (PD) and transimpedance amplifier (TIA). A 12.5 Gb/s bit error rate tester (BERT) is used to perform a clocked comparison of the two received signals, producing a random string of bits. Two variable attenuators (ATT1, ATT2) are used to control the power of the noise signal, and compensate for loss mismatch between the two arms.

in a low-noise erbium-doped fiber amplifier (MPB EFA-R35W). A fiber polarization splitter divides the noise into independent, identically distributed, orthogonally polarized noise signals that are separately detected in a pair of matched photoreceivers (Discovery DSC-R402). Each photoreceiver consists of a photodiode with responsivity of $\mathscr{R} = 0.8$ A/W followed by a transimpedance amplifier with a gain of 500 V/A. The photoreceivers have an electrical bandwidth of 11 GHz, and the transimpedance amplifiers are AC coupled with a cut-on frequency of 30 kHz. Variable optical attenuators were used to adjust the total noise power, and also to balance the noise power in the two orthogonal polarization arms. Because amplified spontaneous emission is generated in both polarization states with equal intensity, we do not require precise polarization control or tracking in order to maintain an acceptable balance between the two arms of the system. The DC photocurrent in each photodiode was adjusted to be 0.77 mA.

To generate random bits, the two independent noise signals $v_1(t)$ and $v_2(t)$ were connected to the differential logic inputs (X and $\bar{X}$) of a bit error rate tester (BERT). In this configuration, the BERT may be thought of as performing a clocked comparison of the two input signals, producing a logical one when $v_1(t) > v_2(t)$ and a logical zero otherwise. An external 12.5 GHz clock signal supplied to the BERT determines the sampling frequency and bit generation rate. A DC bias voltage may be optionally added to either of the input signals, to control the comparison threshold.

4. Noise Characterization

Fig. 4 compares the computed and measured electrical spectra for one channel of the system. In Fig. 4a, we show the power spectrum of the ASE-ASE beat noise, obtained by numerically computing a self-correlation of the measured optical bandpass filter shape shown in Fig. 3b, i.e., $|H_{\mathrm{BP}}(f)|^2 * |H_{\mathrm{BP}}(-f)|^2$ [25]. Fig. 4b shows the measured spectral response of the photoreceiver, which acts as the lowpass filter in our system, $|H_{\mathrm{LP}}(f)|^2$. The photoreceiver spectral response was measured by exciting the detector with a 200 fs pulses from an 80 MHz modelocked laser system, and observing the resulting 80 MHz comb of spectral lines on an RF spectrum analyzer. The spectra shown in Figs. 4a-b are both normalized to a DC value of 0

#134856 - $15.00 USD Received 9 Sep 2010; revised 19 Oct 2010; accepted 20 Oct 2010; published 26 Oct 2010

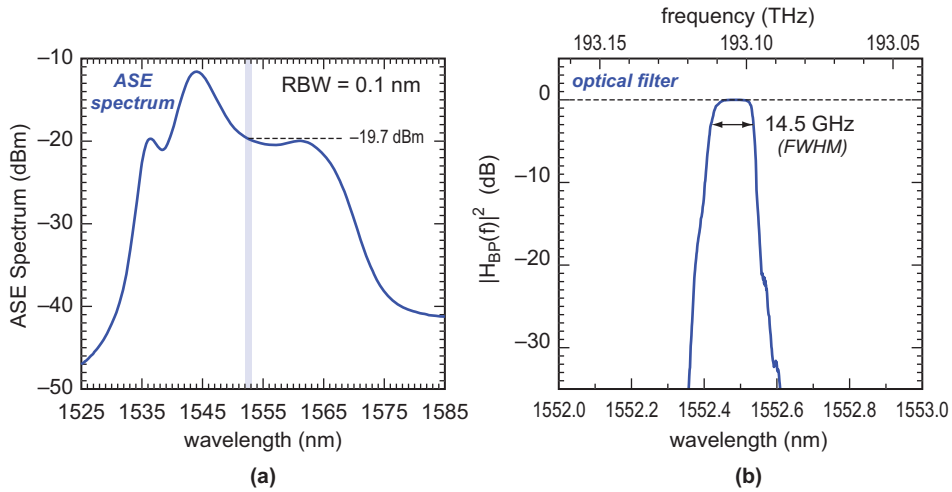

Fig. 3. (a) Optical spectrum of the amplified spontaneous emission produced by the Er/Yb fiber amplifier, measured with a resolution bandwidth (RBW) of 0.1 nm. The shaded band indicates the approximate region where the subsequent optical bandpass filter is located. (b) Reflection spectrum of the fiber-Bragg grating filter, measured using a tunable laser, circulator and power meter. The full-width at half-max (FWHM) bandwidth of the filter was measured to be 14.5 GHz (approximately 0.1 nm.)

dB. Finally, in Fig. 4c, we show the electrical spectrum of the ASE noise from one detector, measured with a resolution bandwidth of 3 MHz. For comparison, we also show the computed noise spectrum obtained by multiplying the two traces from (a) and (b), as described in Eq. (2a), which closely matches the measured spectrum. The computed spectrum was scaled in order to match the DC value observed in the measurement. The final noise spectrum has a bandwidth of 7.5 GHz, which agrees with the result calculated from Eq. (4) using B_{BP} = 14.5 GHz and B_{LP} = 11 GHz. The dotted black line in Fig. 4c shows the background electrical noise spectrum obtained by completely extinguishing the optical signal. Over the frequency range of interest, the electrical noise is more than 40 dB smaller than the optical noise produced by ASE.

Fig. 5 shows characteristic time traces from the two polarization channels in the system, acquired simultaneously on a 20 GHz bandwidth oscilloscope (Tektronix DPO72004B). Although the two signals have nearly identical amplitude distributions, there is no apparent correlation between them. We note that the cable and fiber lengths of the two channels were equalized to within 5 mm (or 25 ps.) The solid curve superposed on the measured voltage histogram shows the best-fit gamma distribution. When performing the fit, the gamma distribution was shifted to have a mean of zero, to account for the fact that the photoreceivers are AC-coupled. The best-fit gamma distribution was obtained with $a = 1.44$, which is in reasonable agreement with the result of 1.37 predicted from Eq. (5b).

#134856 - $15.00 USD Received 9 Sep 2010; revised 19 Oct 2010; accepted 20 Oct 2010; published 26 Oct 2010

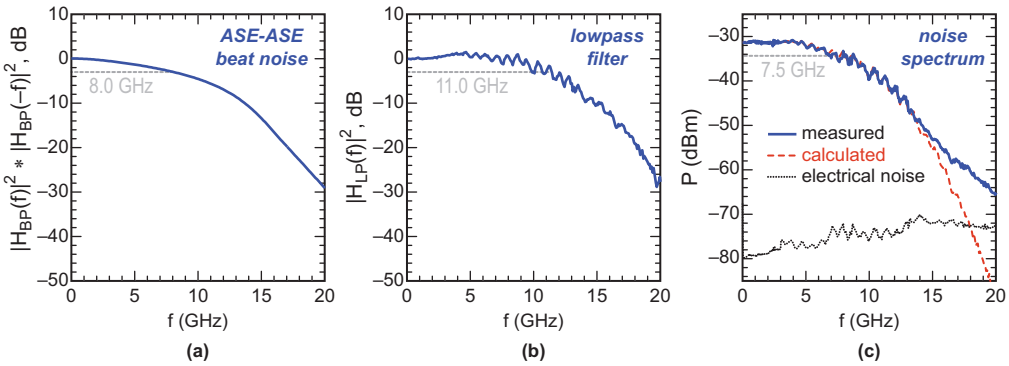

Fig. 4. (a) Electrical spectrum of the ASE-ASE beat noise after square-law detection, estimated by performing a self-convolution of the optical bandpass filter spectrum shown in Fig. 3(b). The spectrum is normalized relative to its DC value. (b) Measured electrical speed of the photoreceiver and transimpedance amplifer, which form an equivalent lowpass filter. (c) Electrical spectrum obtained from one polarization channel, measured directly from one photoreceiver using a resolution bandwidth (RBW) of 3 MHz. The signal exhibits a broad, flat noise spectrum with a (single-sided) bandwidth of 7.5 GHz. The dashed red line shows the spectral shape obtained by multiplying and scaling the curves from (a) and (b). The dotted black line indicates the electrical noise obtained by extinguishing the optical signal. Over the frequency range of interest, the electrical noise remains negligible in comparison to the optical noise arising from ASE.

The two independent noise signals $v_1(t)$ and $v_2(t)$ are detected differentially by the bit error rate tester, which assigns a one or zero based on the difference signal $v_1(t) - v_2(t)$. Fig. 5c shows the calculated difference between the two channels and the corresponding statistical distribution of voltages. Unlike the single channels shown in Fig. 5a-b, the differential voltage has a symmetric distribution, with a mean and median of 0. The theoretical distribution was numerically calculated by performing a self-correlation of the gamma distribution shown in Figs. 5a-b. The balanced detection scheme is insensitive to common-mode interference and drift – even if the source power changes, the decision threshold does not need to be adjusted in order to produce an unbiased bit sequence. Although the fluctuations produced here are macroscopic and unpredictable, we note that for cryptographic applications the security of the resulting bit sequence assumes that a would-be adversary does have access to the physical system or intermediate optical or electrical signals.

In addition to acquiring a binary sequence, the BERT reports a running average of the proportion of ones. Prior to acquiring the binary sequence, the variable attenuator (ATT2) was adjusted to set the mark ratio to 0.5000 ± 0.0001. The instrument is limited to a maximum acquisition length of 128 Mbit, which is not long enough to perform all of the statistical tests required for testing randomness. We therefore concatenated data from eight 128 Mbit records to produce a single 10^9 bit sequence used in subsequent statistical testing.

5. Statistical Testing

One of the simplest statistical measures of randomness is the degree of correlation between adjacent (or delayed) bits in the sequence. Fig. 6a plots the normalized correlation as a function of the bit delay k (or time delay τ) for a 10^9-bit random sequence produced by our system. The

#134856 - $15.00 USD Received 9 Sep 2010; revised 19 Oct 2010; accepted 20 Oct 2010; published 26 Oct 2010

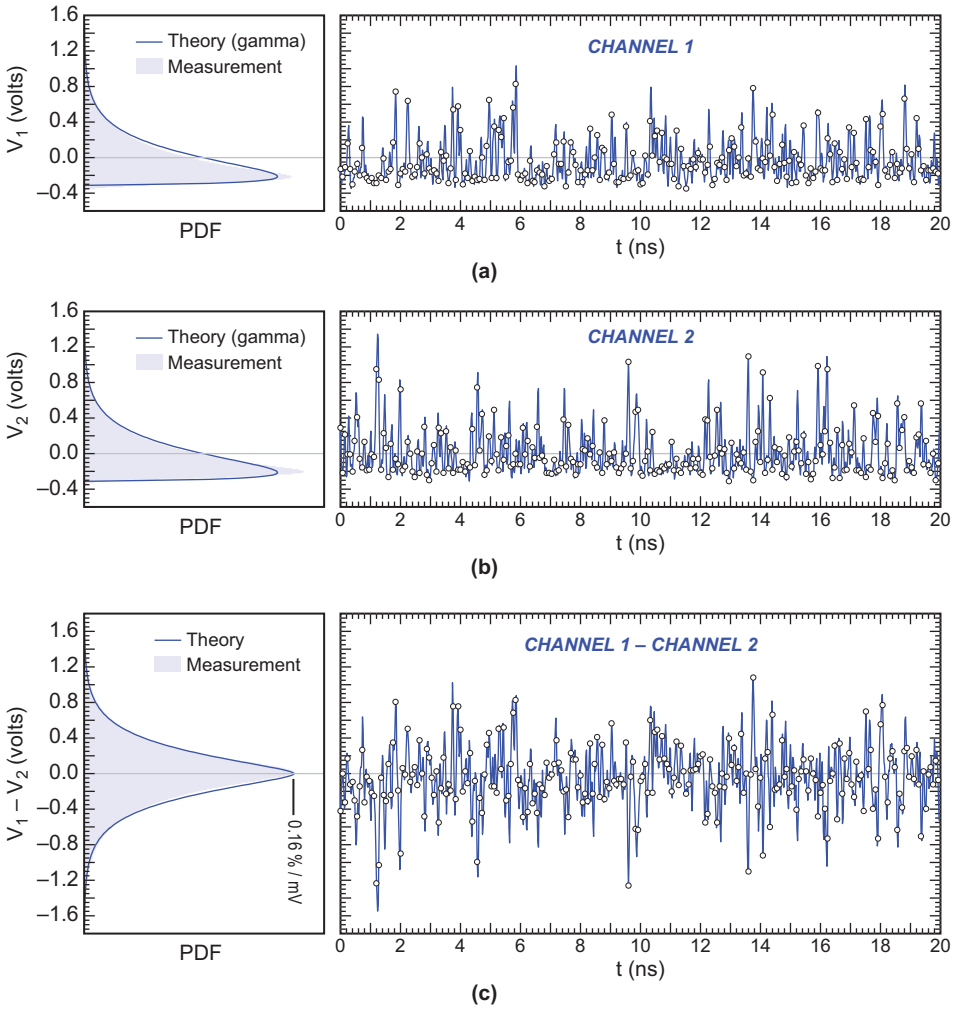

Fig. 5. Representative time traces and statistical histograms measured on a 20 GHz, 50 GS/s digital oscilloscope. The symbols on the time traces inticate the times at which the waveform would be sampled to produce random bits. (a) Single-polarization channel (b) orthogonal polarization channel and (c) differential signal obtained by subtracting two. The theoretical noise distribution shown by the solid curves in (a) and (b) is a best-fit gamma distribution with shape parameter $a = 1.44$ and scale parameter $b = 0.21$ V. The theoretical distribution shown in (c) was calculated by assuming that the two subtracted signals are independent and have identical gamma distributions as obtained in (a) and (b).

#134856 - $15.00 USD Received 9 Sep 2010; revised 19 Oct 2010; accepted 20 Oct 2010; published 26 Oct 2010

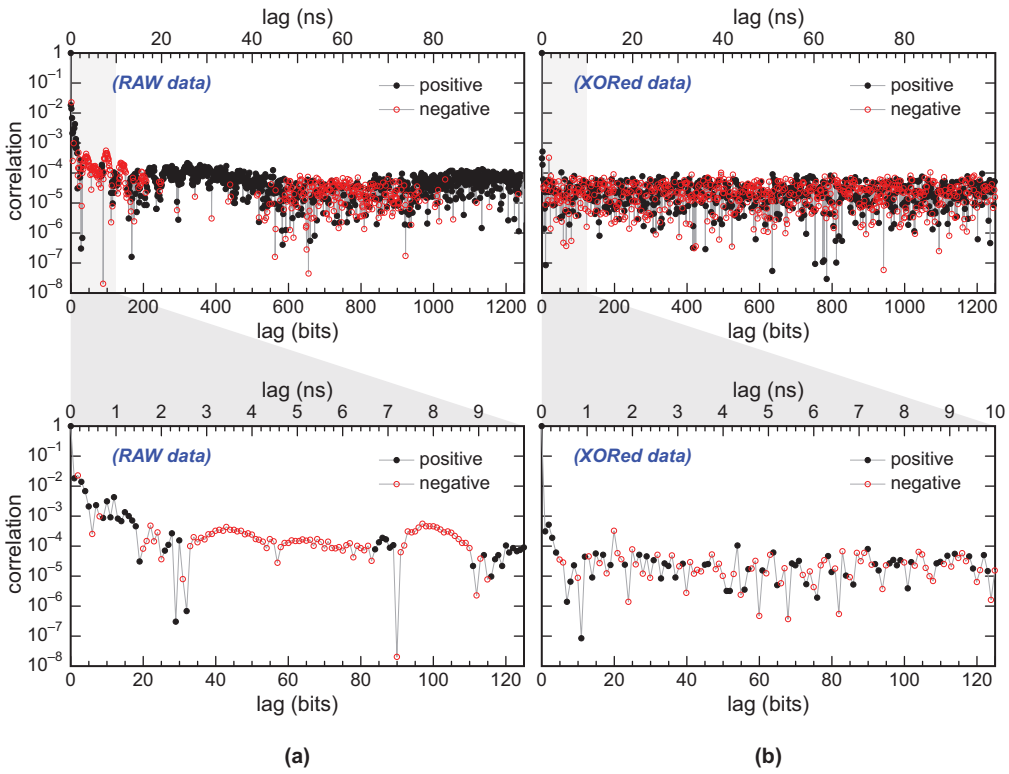

Fig. 6. Normalized binary correlation as a function of lag (a) for the raw bit sequence produced by the experiment and (b) after computing the XOR with a 20-bit delayed copy of the signal. Positive correlation values are indicated with a filled symbol while negative correlations are indicated with open symbols. The correlation was calculated using a 10^9 bit record. For a truly random unbiased 10^9 bit record, one expects to obtain an average normalized correlation of 0 and a standard deviation of the correlation of 3.16×10^{-5} [31].

normalized correlation at lag k was calculated in the following way

$$\rho_k = \frac{\langle b[n]b[n+k]\rangle - \langle b[n]\rangle^2}{\langle b^2[n]\rangle - \langle b[n]\rangle^2}, \tag{8}$$

where $\langle\bullet\rangle$ denotes a statistical average over the N bits of the binary sequence $b[n]$. When computing the average $\langle b[n]b[n+k]\rangle$, the N-bit sequence $b[n]$ is assumed to repeat with a period of N, e.g., $b[N+k]=b[k]$. The correlation ρ_k defined in Eq. (8) is a symmetric function of the lag k, with $\rho_0=1$. For a finite length sequence of N ideal, independent, unbiased bits, the correlation calculated by Eq. (8) has an expected value that decreases as $(-1/N)$ and a standard deviation that decreases as $1/\sqrt{N}$ [31]. For $N=10^9$, we therefore expect the correlation for $k\neq0$ to be statistically centered about 0 with a standard deviation of 3.16×10^{-5}.

As shown in Fig. 6a, the raw data produced by our system exhibits a small, but statistically significant correlation, especially for small lags. There is also a small but clearly discernible ringing pattern in the correlation, which slowly alternates between positive and negative as a function of k, even for large lags. Without the XOR processing, the small but statistically significant correlation seen in Fig. 6a would cause the raw bit sequence to fail several of the statistical tests.

#134856 - $15.00 USD Received 9 Sep 2010; revised 19 Oct 2010; accepted 20 Oct 2010; published 26 Oct 2010

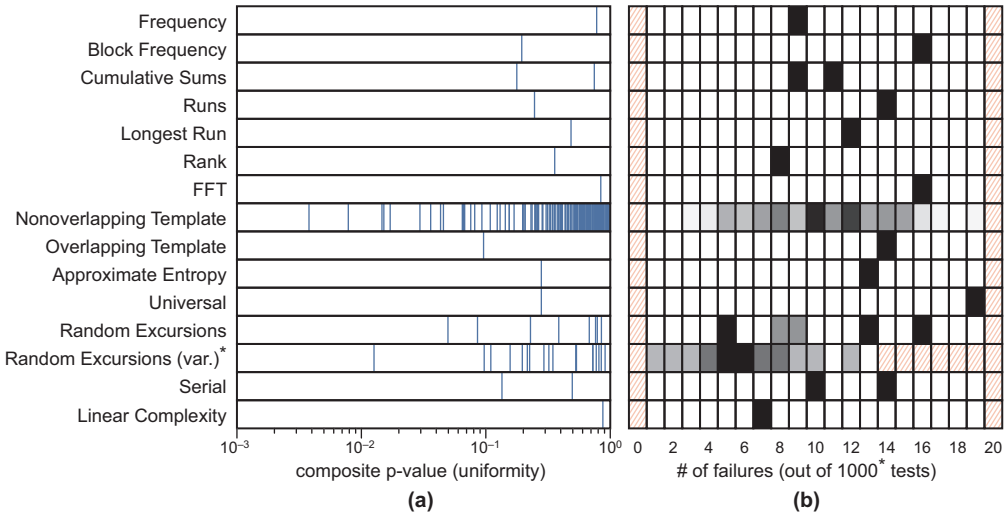

Fig. 7. Summary of test results obtained from the NIST statistical test suite (STS-2.1) [32] applied to a 10^9 bit record obtained from the XORed data set. The NIST test suite comprises 15 types of tests, some of which return multiple results. (a) The composite p-values for each of the statistical tests and (b) the number of "failures" out of 1000 trials. For a truly random bit sequence, the p-values should be uniformly distributed on the interval [0,1], and the number of failures should follow binomial distribution with $N = 1000$ and $\alpha = 0.01$. For tests that return multiple results, all composite p-values are plotted in (a), and (b) shows a gray-scale histogram reflecting the number of failures out of 1000*. The passing criteria are that all of the computed p-values must exceed 0.0001 and each test must yield between 1 and 19 failures out of 1000 trials. *The random excursions variant test is applied to only 561 records, and may have no more than 13 failures.

One simple and common way to decrease the correlations of a random bitstream is to form a new sequence by taking the exclusive or (XOR) between independently acquired sequences [5,6,17,19]. For two identically distributed sequences with a mark-ratio of p and correlation of ρ_k, the binary sequence obtained by computing the XOR will have a mark ratio and correlation of

$$p' = 2p(1-p), \qquad \rho'_k = \rho_k(1-p')(1-2p'+\rho_k p'). \tag{9}$$

If the original sequences are unbiased, then the XOR process will produce an unbiased sequence with new correlation $\rho'_k = \rho_k^2/4$. In practice, we have found that the statistical properties can be improved by taking the XOR between the original sequence and a delayed copy of itself. Delays as small as 20 bits were found to be sufficient to produce a sequence that passes all of the statistical tests for randomness. Fig. 6b plots the normalized binary correlation for the XORed data sequence $b[n] \oplus b[n-20]$. The resulting sequence exhibits a correlation near the statistical noise level, with no discernible pattern or trend. Although we computed the XOR using off-line postprocessing, it could easily be implemented in real-time using simple high-speed logic operations. The lagged XOR process does not require more than 20 bits of delay, and does not reduce the generation rate.

We also evaluated the statistical properties of the random process using the NIST statistical test suite for cryptographic random number generators [32]. The NIST test suite contains 15 types of statistical tests, some of which contain multiple sub-tests. Each test is applied to a 1 Mbit sequence and returns a "p-value" that, for a truly random bit sequence, would be uniformly distributed between 0 and 1. The NIST test suite applies each test to 1000 sequences (a total

#134856 - $15.00 USD Received 9 Sep 2010; revised 19 Oct 2010; accepted 20 Oct 2010; published 26 Oct 2010

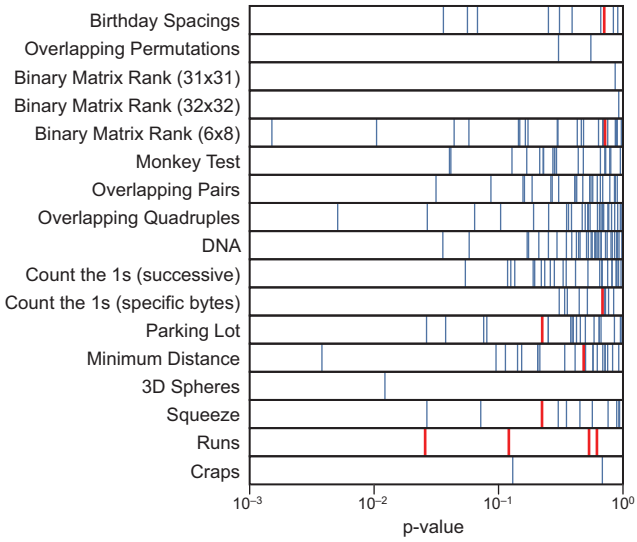

Fig. 8. Summary of test results obtained from the Diehard test suite applied to a 74×10^6 bit record obtained from the XORed data set. For tests that return multiple p-values, all are shown. For tests that compute a composite p-value by applying the Kolmogorov-Smirnov (K-S) test, the resulting p-value is indicated in red. In order to pass the tests, all p-values (or, where appropriate, the composite K-S p-value) must exceed 0.0001.

of 10^9 bits) and then computes a single composite p-value to assess whether the constituent p-values are uniformly distributed. For a truly random sequence, the composite p-value should also be uniformly distributed between 0 and 1. The composite p-values must all exceed 10^{-4} in order to pass the NIST test. Furthermore, of the 1000 individual p-values obtained for each test, no fewer than 1 nor more than 19 may fall below the threshold of $\alpha = 0.01$. Fig. 7 plots the results of the NIST tests applied to the 10^9 bit XORed data sequence. For tests that produce multiple composite p-values, all are shown in Fig. 7a. The number of tests (out of 1000) with $p < 0.01$ is plotted in Fig. 7b. For tests that produce multiple results, the numbers are shown as a grayscale histogram. The XORed data set passes all of the NIST statistical tests.

We also confirmed that the XORed data set passes all the tests in the Diehard statistical suite [33]. The Diehard suite comprises 17 different statistical tests, some of which require up to 74 Mbits of data. As with the NIST tests, each of the tests returns a p-value that, for a random sequence, would be uniformly distributed between 0 and 1. For some tests, the Diehard suite computes a composite p-value using the Kolmogorov-Smirnov (K-S) test to asses the degree of uniformity. In Fig. 8 we plot the results of the Diehard tests. p-values obtained from the K-S test are indicated by thick red lines. Where available, the individual p-values from which the composite was calculated are shown by the thin blue lines. In order to pass each test, the computed p-values (or, where available, the K-S p-value) must all exceed 10^{-4}.

It must be emphasized that while statistical testing has a role in evaluating random number generators, it should not be the sole qualifying criterion for all applications. The speed, simplicity, cost, long-term stability, and security are all features that cannot be assessed using standard statistical tests. Moreover existing statistical tests cannot distinguish between different physical sources of randomness. Depending on the specific needs of the application, new tests may be needed to judge the suitability of a given method of random number generation. At a fundamental level, Pironio et al. recently described an experimental approach to certifying the

#134856 - $15.00 USD Received 9 Sep 2010; revised 19 Oct 2010; accepted 20 Oct 2010; published 26 Oct 2010

randomness of a measurement by testing Bell's inequality [34]. Apart from this, the goal of quantifying randomness using non-statistical, experimental measurements remains difficult.

6. Improving Generation Rate with Analog-to-Digital Conversion

A few groups have recently demonstrated extremely fast random bit generation using chaotic lasers and high-speed analog-to-digital converters (ADCs) [21–23]. Instead of applying a simple threshold comparison (as was done here), these systems utilize the output of an ADC in order to produce multiple bits per sample. In order to generate sequences that pass all of the requisite statistical tests, these methods all employ some form of digital processing that include discarding the most significant bits. The ultimate speed that can be achieved using such methods is not known, but will depend primarily on the cost and complexity of postprocessing that is deemed acceptable. As noted by others [23], it is unclear to what extent the high-speed chaotic optical signal contributes to the performance, in comparison to the intrinsic noise of the ADC converter, which can often dominate the least significant bits [35].

For the purpose of comparison, we investigated using a high-speed ADC with the spectrally-sliced ASE noise source reported here. The time traces shown in Fig. 5a-b were collected on a 20 GHz, 50 GS/s, 8-bit oscilloscope. Using the 8-bit signed integers $x[n]$ (in two's-complement format) taken from these records, we computed a 9-th order discrete derivative (using 32-bit, two's-complement arithmetic), and retained only the 8 least significant bits of the resulting sequence [22]:

$$\begin{aligned} y[n] = \big(&x[n] - 9x[n-1] + 36x[n-2] - 84x[n-3] + 126x[n-4] - 126x[n-5] \\ &+ 84x[n-6] - 36x[n-7] + 9x[n-8] - x[n-9]\big) \ \texttt{\&\ 0x000000FF}. \end{aligned} \tag{10}$$

In this way, we produce a new sequence of unsigned 8-bit integers, $y[n]$ at a rate of 50 GHz, for a cumulative random generation rate of 400 Gb/s (or 800 Gb/s if one considers both orthogonal polarization channels.) The resulting sequence was confirmed to pass all of the standard NIST and Diehard tests for randomness. Next, we completely extinguished the optical signal and performed the same process using only the background electrical noise present in our system. The resulting sequence *also* passed all of the NIST and Diehard statistical tests.

This experiment suggests that a chaotic laser or other optical noise source is not an essential ingredient for such methods: other sufficiently random electrical input signals applied to an ADC (including the intrinsic electrical noise and sampling noise) can produce statistically random bits, when digital processing is employed. Using the postprocessed least significant bits from an ADC to generate random numbers is feasible, but more costly and less practical than the ASE-based system described here, which is comprised entirely of telecom-grade components commonly found in optical networks.

7. Conclusion

We demonstrated a 12.5 Gb/s random number generator based on threshold detection of filtered amplified spontaneous emission by a high-speed photoreceiver. The amplified spontaneous emission noise is shown to be significantly stronger than the electrical background noise, and the measured statistical distributions and noise spectra show a close agreement with theory. Unlike earlier reported optoelectronic random number generators that are limited in speed by photon counting electronics or laser dynamics, this system is limited primarily by the speed of available photoreceivers. This random number generation method is therefore guaranteed to keep pace with ongoing advances in digital optical communication systems, as both rely on the same key optoelectronic components. The system uses telecom grade filters, fiber amplifiers, and detectors, and could easily be extended to multiple wavelength channels, each of which

#134856 - $15.00 USD Received 9 Sep 2010; revised 19 Oct 2010; accepted 20 Oct 2010; published 26 Oct 2010

would generate independent random sequences in parallel. The resulting random bit sequence passes the most widely accepted statistical tests used to evaluate cryptographic random number generators.

8. Acknowledgements

The authors thank Elizabeth Rogers-Dakin (Optical Air Data Systems) for providing the Er/Yb-doped fiber amplifiers used to generate ASE noise and Allen Chopyk (Tektronix) for providing the digital oscilloscope used to measure the high-speed waveforms. This work is supported by DOD MURI grant (ONR N000140710734).

#134856 - $15.00 USD Received 9 Sep 2010; revised 19 Oct 2010; accepted 20 Oct 2010; published 26 Oct 2010