Implementation of 140 Gb/s true random bit generator based on a chaotic photonic integrated circuit

Apostolos Argyris,* Stavros Deligiannidis, Evangelos Pikasis, Adonis Bogris, and Dimitris Syvridis

Department of Informatics and Telecommunications, University of Athens, Panepistimiopolis, Ilisia, 15784, Greece
**argiris@di.uoa.gr*

Abstract: In the present work a photonic integrated circuit (PIC) that emits broadband chaotic signals is employed for ultra-fast generation of true random bit sequences. Chaotic dynamics emerge from a DFB laser, accompanied by a monolithic integrated 1-cm long external cavity (EC) that provides controllable optical feedback. The short length minimizes the existence of external cavity modes, so flattened broadband spectra with minimized intrinsic periodicities can emerge. After sampling and quantization - without including optical de-correlation techniques and using most significant bits (MSB) elimination post-processing - truly random bit streams with bit-rates as high as 140 Gb/s can be generated. Finally, the extreme robustness of the random bit generator for adaptive bit-rate operation and for various operating conditions of the PIC is demonstrated.

OCIS codes: (140.1540) Chaos; (130.3120) Integrated optics devices; (320.7080) Ultrafast devices

References and links

1. N. Ferguson, and B. Schneier, *Practical Cryptography* (John Wiley & Sons, 2003).
2. http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf (2001).
3. 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**(6), 521–528 (1997).
4. J. T. Gleeson, "Truly random number generator based on turbulent electroconvection," Appl. Phys. Lett. **81**(11), 1949 (2002).
5. 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**(4), 403–409 (2003).
6. C. Tokunaga, D. Blaauw, and T. Mudge, "True random number generator with a metastability-based quality control," IEEE J. Solid-state Circuits **43**(1), 78–85 (2008).
7. J.-L. Danger, S. Guilley, and P. Hoogvorst, "High speed true random number generator based on open loop structures in FPGAs," Microelectron. J. **40**(11), 1650–1656 (2009).
8. J. F. Dynes, Z. L. Yuan, A. W. Sharpe, and A. J. Shields, "A high speed, post-processing free, quantum random number generator," Appl. Phys. Lett. **93**(3), 031109 (2008).
9. 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**(3), 312–314 (2010).
10. M. A. Wayne, and P. G. Kwiat, "Low-bias high-speed quantum random number generator via shaped optical pulses," Opt. Express **18**(9), 9351–9357 (2010).
11. R. Lang, and K. Kobayashi, "External optical feedback effects on semiconductor injection laser properties," IEEE J. Quantum Electron. **16**(3), 347–355 (1980).
12. J. Mork, B. Tromborg, and J. Mark, "Chaos in semiconductor lasers with optical feedback: theory and experiment," IEEE J. Quantum Electron. **28**(1), 93–108 (1992).
13. 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," Nat. Photonics **2**(12), 728–732 (2008).
14. K. Petermann, *Laser diode modulation and noise,* (Kluwer Academic Publ., 1991).
15. I. Reidler, Y. Aviad, M. Rosenbluh, and I. Kanter, "Ultrahigh-speed random number generation based on a chaotic semiconductor laser," Phys. Rev. Lett. **103**(2), 024102 (2009).
16. I. Kanter, Y. Aviad, I. Reidler, E. Cohen, and M. Rosenbluh, "An optical ultrafast random bit generator," Nat. Photonics **4**(1), 58–61 (2010).

#130312 - $15.00 USD Received 17 Jun 2010; revised 20 Jul 2010; accepted 20 Jul 2010; published 18 Aug 2010

17. 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**(6), 5512–5524 (2010).
18. A. Argyris, M. Hamacher, K. E. Chlouverakis, A. Bogris, and D. Syvridis, "Photonic integrated device for chaos applications in communications," Phys. Rev. Lett. **100**(19), 194101 (2008).
19. A. Argyris, E. Grivas, M. Hamacher, A. Bogris, and D. Syvridis, "Chaos-on-a-chip secures data transmission in optical fiber links," Opt. Express **18**(5), 5188–5198 (2010).
20. J. Ohtsubo, *Semiconductor Lasers: Stability, Instability and Chaos* (Springer-Verlag, 2006).
21. 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 (2010).

1. Introduction

Random number generators play a fundamental role in most algorithms and systems for cryptographic applications [1,2]. Communications based on secret and public key cryptography, user authentication, as well as lottery-based applications rely on the quality of the randomness provided by these generators. Two types of random number generators can be distinguished, namely true random number generators (TRNGs) and pseudorandom number generators (PRNGs) [2]. TRNGs produce random bits from random physical phenomena or noise sources [3–8]. Such non-deterministic generators have limited efficiency in number generation rates due to limitations of the mechanisms for extracting bits from the physical procedures. On the contrary, PRNGs are initiated by a relatively short key (seed) and their output is expanded into a long sequence of random bits using computational deterministic algorithms [1]. PRNGs were viewed until recently as a largely solved problem, but emerging technologies and advanced computational requirements start to change the game. In cases where the "entropy pool" - from which the seed comes up - is inadequate, no matter how strong the encryption is, a malicious hacker could succeed in guessing correct. So, how can computers produce or exploit truly random numbers that can't be guessed or replicated? And how can – at the same time – the bit rate generation rise significantly in order to support challenging modern applications, such as demanding Monte Carlo simulations, stochastic modeling, security of cluster computing, real time data encryption, etc.?

Very recently, research in quantum noise TRNGs demonstrated configurations that could increase significantly the bit-rate generation efficiency, potentially over 100 Mbps [9,10]. However, even such bit-rates are much slower than the ones achieved by the recently proposed technique using broadband chaotic signals emitted from semiconductor lasers (SLs) with optical feedback [11,12]. In the pioneering work of [13] a 1.7 Gb/s TRNG was presented based on the binary digitization of two independent chaotic SLs, finally combined under a XOR operation. A single-laser chaotic signal could not be adopted as the random source due to the periodicities of the external cavity modes (ECMs) of the chaotic waveform [14]. A severe drawback in this configuration is the accurate determination of the bit decision voltage required. In more efficient schemes that have been proposed since then, the random bit sequence is formed by considering only several least significant bits (LSBs) of the 8-bit analog-to-digital (A/D) converted signal. In these works either advanced electrical post-processing offline methods - based on either the difference between delayed 8-bit samples [15] or high-order derivatives [16] using offline memory buffers for intermediate sequences storage - or optical de-correlation techniques - using a relatively complex configuration with coupled lasers for chaotic signal bandwidth enhancement and ECM suppression [17] - have been employed in order to claim an ultra-high bit rate TRNG.

In this work, we demonstrate the first compact real-time true random bit generator (TRBG) that exploits broadband chaotic signals emitted by a photonic integrated circuit (PIC). The proposed generator is simpler than the existing configurations and consists of the PIC, a photodetector and a 40GSa/s oscilloscope, without including any optical de-correlation methods. Depending on the operating conditions of the PIC and by using MSB elimination post-processing, real time bit sequences extracted from the oscilloscope Ethernet output port, with verified randomness and rates as high as 140Gb/s become available. The proposed

#130312 - $15.00 USD Received 17 Jun 2010; revised 20 Jul 2010; accepted 20 Jul 2010; published 18 Aug 2010

configuration provides significant advances in terms of simplicity, performance and especially robustness.

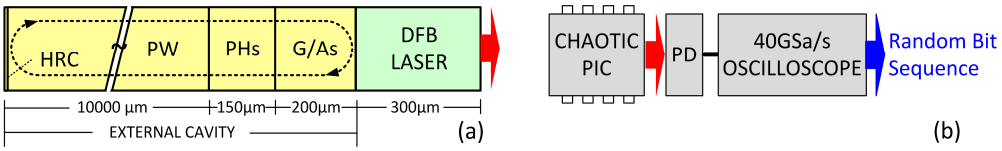

Fig. 1. (a) Schematic of the photonic integrated circuit (PIC). (b) A true random bit generator (TRBG) based on the emitted chaotic signal from the PIC.

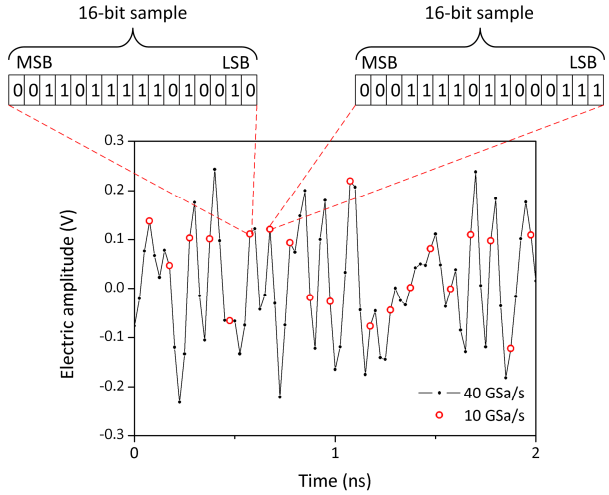

Fig. 2. Timetrace of the chaotic analog signal. The sampling rate is set to 40GSa/s (black dots) while only 10GSa/s (red circles) are considered for the output of the TRNG. Only *k* LSBs out of the 16-bit digitized representation of each sample is included in the final output sequence.

2. Experimental setup

The PIC employed in this work has been specifically designed and fabricated for providing fully controllable and stable chaotic optical signals at 1556nm with broadband microwave spectral characteristics over 10GHz. As shown in Fig. 1a, it consists of a DFB laser followed by an integrated 1cm passive waveguide (PW) cavity with a highly reflective coated (HRC) end; an active gain/absorption section (G/As) that controls the optical feedback of the cavity and a passive phase section (PHs) that controls the phase of the generated optical field are also included within the cavity [18]. The chaotic signal generation is based on the delayed optical feedback effect [11,12]. The proposed TRBG scheme is shown in Fig. 1b. The chaotic optical signal from the PIC is fed through its fiber pigtail to a HP11982A 15GHz photoreceiver (PD) after optical isolation in order to eliminate any residual reflectivity that would disturb the PIC operation. The converted electrical signal is sent finally to a real-time oscilloscope (Agilent 81204B) with 40GSa/s sampling rate and 12 GHz bandwidth. The oscilloscope's 8-bit A/D converter, along with the internal 16-bit digital-to analog convertor (DAC) and the rest processing units, provides a "word-type", noise-enhanced, 16-bit output binary sequence for each sample. An external down-sampling to 10GSa/s is applied – i.e. one out of each four samples is considered – in order to eliminate any effect of interpolation samples of the oscilloscope. In such a way the initial bandwidth of the signal is preserved. The down-sampling operation in the chaotic timetrace is shown in Fig. 2. The number (*k*) of the LSBs retained in each sample of the output sequence determines the final bit rate generation.

#130312 - $15.00 USD Received 17 Jun 2010; revised 20 Jul 2010; accepted 20 Jul 2010; published 18 Aug 2010

3. Analog signal generation

The biasing conditions of the PIC determine the signal's chaotic complexity, spectral distribution and bandwidth to a great extend [19,20]. The DFB laser section - with a threshold current value I_{th} = 25mA – provides chaotic signals that include low frequency fluctuations (LFFs) [20] when biased up to 28mA. Beyond that values and for EC feedback ratio (i.e. the ratio of the DFB laser's optical output that is re-injected after running a roundtrip path in the integrated external cavity) above P_f = 0.5%, chaotic signals with powerful broadband spectra emerge. Two cases of P_f have been examined in this work, by appropriately biasing the G/As. In the G/As unbiased case, P_f = 1.6%, while when G/As is biased with 0.1mA (0.733mV), P_f = 3.3%. The microwave spectra that correspond to these two feedback conditions, for different DFB laser current values, are presented in Fig. 3. ECMs with spacing 3.3GHz – that correspond to the EC length – appear only in the P_f = 3.3% case, while suppressed significantly when increasing the biasing DFB laser current (Fig. 3b). The prerequisite for a potential analog signal to seed successfully an ultra-fast TRBG is a broad and flat spectrum, without periodicities. Under these specifications, the most prominent operating condition of the PIC is expected from signals with a spectral distribution of Fig. 3a, at high current values (e.g. 50mA case).

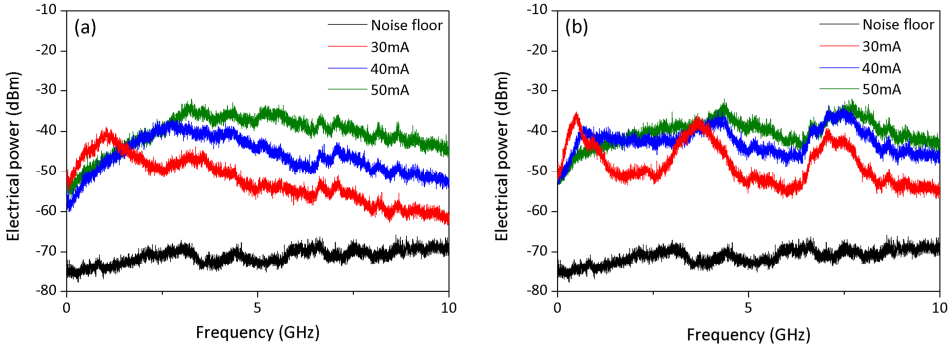

Fig. 3. Spectral distribution of the electrical output of the chaotic PIC after photodetection, for various DFB laser biasing currents (30mA, 40mA and 50mA) and two different cases of internal optical feedback strength: (a) 1.6% and (b) 3.3%.

4. Random bit generation and verification

In order to claim and prove the randomness of a bit sequence strict conditions must be fulfilled. The most representative statistical tests performed for this reason are included in the NIST SP800-22(rev.1a, April 2010) test suite [21] which is adopted in this work. 1000 samples of 1Mbit sequences – constructed by the appropriate number of the k LSBs adopted in each case – are evaluated. Pass criteria are determined by the sequence length and the significance level. A significance level α = 0.01 is set for the p-values of each sequence test, with a desirable uniformity P-value larger than 0.0001. For the 1000 samples, the proportion of sequences that satisfy p-value > α, is estimated to be 0.99 ± 0.0094.

A randomness mapping of the PIC-based TRBG in terms of operating conditions is performed in Fig. 4. The randomness is verified when all 15 statistical tests of the NIST test suite are passed. The characterization has been performed versus the biasing laser current - with a 1mA analysis – and the number of LSBs of each sample included in the output sequence – from k = 1 to k = 16 – for the two optical feedback conditions presented in Fig. 3a and 3b. The complete absence of ECMs and the powerful broadband spectral distribution of the chaotic signal, for the case of P_f = 1.6% (Fig. 3a) and for laser biasing current above 47mA, allows the most favorable performance. All NIST tests are passed, even when including 14 LSBs, which is translated into bit-rate generation of 140Gb/s. A representative analysis of the NIST statistical tests results, for the worst value of the obtained p-values for

#130312 - $15.00 USD Received 17 Jun 2010; revised 20 Jul 2010; accepted 20 Jul 2010; published 18 Aug 2010

each test, is presented in Table 1. Lower current values alter the chaotic spectral profile, either by reducing its bandwidth or by revealing ECM periodicities. The adoption of gradually decreased number of LSBs in each sample allows even now a random bit stream with verified randomness. However, in all cases – even at the PIC's LFF operating region just above threshold – a minimum 90Gb/s TRBG is guaranteed. As shown in Fig. 3b, the increase of the optical feedback strength to 3.3% results in evident ECMs. The corresponding randomness mapping for this case is shown in Fig. 4b. For large laser current values ECMs are partially suppressed, permitting the TRNG to operate successfully at bit-rates between 80Gb/s and 120Gb/s. Even at lower laser biasing current values and albeit the apparent ECM existence TRNG can be claimed at bit-rates as high as 70Gb/s.

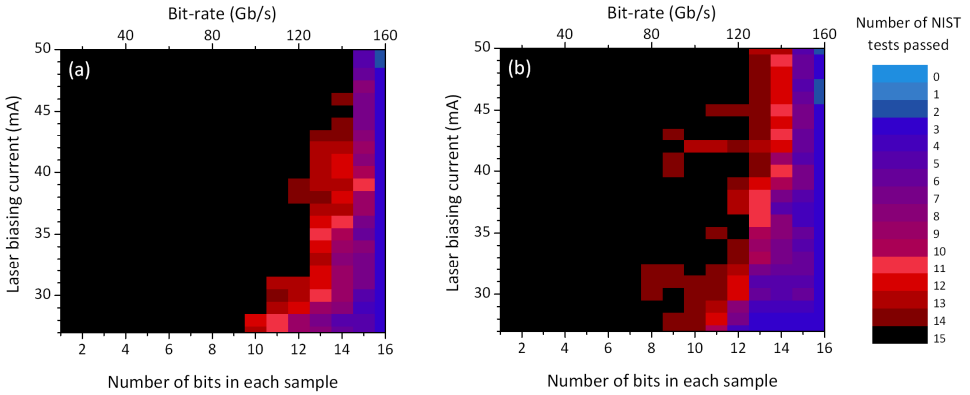

Fig. 4. Mapping of the TRBG performance in terms of bit-rate and number of NIST randomness tests passed. The characterization has been performed vs. the biasing laser current and the number of LSBs of each sample included in the output sequence, for (a) P_f = 1.6% and (b) P_f = 3.3%. Black color grade regions designate operating conditions where all NIST randomness tests are successful.

Table 1. Results of NIST SP800-22(rev.1a) statistical test suite for the case of DFB laser current 48mA, P_f = 1.6% and k = 14 (10GS/s). The final TRBG rate is 140Gb/s.

STATISTICAL TEST	P-VALUE (min)	PROPORTION	RESULT
Frequency	0.375313	0.986	Passed
Block frequency	0.674543	0.990	Passed
Runs	0.773405	0.988	Passed
Longest Run	0.087162	0.988	Passed
Rank	0.291091	0.991	Passed
Discrete Fourier transform	0.134355	0.984	Passed
Non-overlapping templates	0.002186	0.986	Passed
Overlapping templates	0.989425	0.990	Passed
Universal	0.705466	0.991	Passed
Linear complexity	0.883171	0.989	Passed
Serial	0.123038	0.995	Passed
Approximate entropy	0.607993	0.993	Passed
Cumulative sums	0.514124	0.991	Passed
Random excursions	0.023140	0.9886	Passed
Random excursions variant	0.015993	0.9869	Passed

Several useful conclusions emerge from the performance of the presented chaotic PIC-based TRBG. The laser intensity histogram independently of the PIC's operating conditions is not symmetrical; even though approaches to a Gaussian profile for the optimal operating conditions presented in Table 1, with skewness and kurtosis values measured equal to 0.07 and 2.52, respectively. This is translated in a bias in the first m MSBs of each sample. By optimizing the operating conditions – and thus the analog signal distribution within the 16-bit quantized window – an attempt to minimize the m value is performed. This has been achieved, for example, for the conditions of Table 1, where m = 2. Less symmetrical histogram

#130312 - $15.00 USD Received 17 Jun 2010; revised 20 Jul 2010; accepted 20 Jul 2010; published 18 Aug 2010

representations of the chaotic signal just require the exclusion of a further increased number of *m* values in order to obtain a verified TRBG. Such a performance establishes the proposed configuration as a robust, compact device for TRBG with an ultra-fast adaptive bit-rate performance.

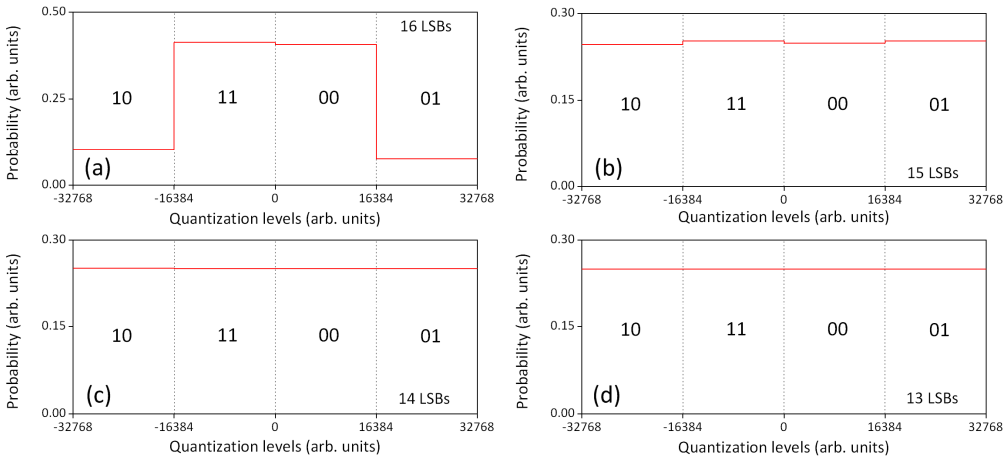

Fig. 5. Probability distributions of sampled multi-bit data, when including (a) all 16 output bits, (b) 15 LSBs, (c) 14 LSBs and (d) 13 LSBs, for the operating conditions of Table 1.

In Fig. 5 the probability distributions of sampled multi-bit data, when including (a) all 16 output bits, (b) 15 LSBs, (c) 14 LSBs and (d) 13 LSBs, for the operating conditions of Table 1, are presented. Each graph is split in 4 regions with the first two bits cases (10, 11, 00 and 01) and the integral of all bits in each region is calculated. Especially in Fig. 5a case where no MSBs have been eliminated, it is clear that the sampled chaotic waveform is not completely uniform. On the contrary, when considering less than 15 LSBs, the distribution histogram becomes completely uniform leading to a TRBG with verified randomness.

5. Conclusions

A robust chaotic PIC-based TRBG is presented, capable of generating random bit sequences at ultra-fast bit-rates. Under optimized operating conditions, chaotic signals with flat broadband spectra and minimized periodicities emerge. After analog signal sampling, quantization and MSBs elimination post-processing, verified random bit sequences at 140 Gb/s rates are produced. Even without optimizing the PIC's operating conditions and achieving a symmetric distribution a TRBG can also be claimed with an adaptive decreased bit-rate performance.

Acknowledgement

The PICs used in this work were developed under the EU FP6-IST-34551 PICASSO project within the Fraunhofer Institute for Telecommunications facilities, Heinrich-Hertz-Institute, 10587, Berlin, Germany.

#130312 - $15.00 USD Received 17 Jun 2010; revised 20 Jul 2010; accepted 20 Jul 2010; published 18 Aug 2010