Generation of High-Entropy, Bandwidth-Enhanced Chaos in Semiconductor Lasers for Tbit/s Random Bit Generation

1st Chin-Hao Tseng
Department of Information and Computer Sciences
Saitama University
Saitama, Japan
Department of Photonics
National Cheng Kung University
Tainan, Taiwan
chtseng0828@mail.saitama-u.ac.jp

2nd Atsushi Uchida
Department of Information and Computer Sciences
Saitama University
Saitama, Japan
auchida@mail.saitama-u.ac.jp

3rd Sheng-Kwang Hwang
Department of Photonics
National Cheng Kung University
Tainan, Taiwan
Meta-nanoPhotonics Center
National Cheng Kung University
Tainan, Taiwan
skhwang@mail.ncku.edu.tw

***Abstract*—Fast and reliable random numbers are essential for a wide range of security-critical and computationally demanding applications, including cryptography, artificial intelligence, and large-scale simulations. To achieve random number generation with high throughput, the generation of broadband, high-entropy physical sources that exhibit strong unpredictability and minimal deterministic structure is required. In this work, we generate bandwidth-enhanced chaos using semiconductor lasers, achieving a standard bandwidth of 76.8 GHz and an entropy rate of 1.7 Tbit/s, which supports random bit generation at 1.536 Tbit/s with only simple post-processing. These results indicate that the proposed chaos-generation approach provides a potential route to realizing fast random number generators in real time, with broad applicability in modern information technologies.**

***Index Terms*—Semiconductor lasers, broadband chaos, high-entropy sources, random bit generation**

I. INTRODUCTION

The rapid expansion of modern information technologies has increased the need for fast and reliable random number generation, as true randomness is essential for security-critical and AI-related computational applications, including secure communication, secure key distribution [1], [2], generative adversarial networks [3], and large-scale machine learning. With data rates and AI-related computational workloads continuing to rise, future digital systems will require high-speed random number generators capable of producing high-quality randomness.

Although algorithmic pseudo-random number generators are fast and widely used, their deterministic nature may limit their suitability for security-sensitive scenarios and may constrain performance in massively parallel computing environments [4] due to hidden correlations among the generated sequences. In contrast, physical random number generators derive randomness from high-entropy physical sources, yielding non-reproducible and inherently unpredictable outputs. These characteristics make them highly attractive for security-oriented and high-performance computing applications. Consequently, the development of physical architectures capable of generating broadband, high-entropy sources for fast random bit generation (RBG) is of significant importance.

Chaotic oscillations in semiconductor lasers are among the most promising entropy sources for fast RBG, owing to their rapid phase dynamics and inherently irreproducible behavior. Numerous studies have explored various architectures based on semiconductor lasers to achieve bandwidth enhancement of chaos for fast RBG, including external optical feedback [5], cascaded injection [6], external modulation [7], and laser networks [8]. These efforts have improved the chaos bandwidth to approximately 40 GHz [6], [7]. Nevertheless, the entropy throughput attainable at this bandwidth remains insufficient to support Tbit/s-level RBG rates, as the achievable bandwidth directly constrains the entropy rate of the source [9].

To overcome the entropy throughput limitation, several studies have applied complex offline post-processing techniques, such as high-order differentiation [10] or bit-order-reversal operations [6], to remove inter-sample correlation when oversampling, thereby enabling Tbit/s RBG rates. However, these methods inevitably increase hardware overhead and processing latency, making real-time implementation challenging. Achieving high entropy throughput directly from the physical source for RBG at Tbit/s rates, without relying on heavy post-processing, remains an open and critical issue.

In this work, we achieve broadband chaos generation through the beat note between the chaotic output of a semiconductor laser and an optical frequency comb. The resulting bandwidth-enhanced chaos exhibits a standard bandwidth of 76.8 GHz and a flat spectral distribution, with a verified entropy rate of 1.7 Tbit/s. Furthermore, by applying a simple delayed exclusive-OR operation [11] before extracting the least significant bits of the digitized chaos source, an RBG rate of 1.536 Tbit/s is achieved.

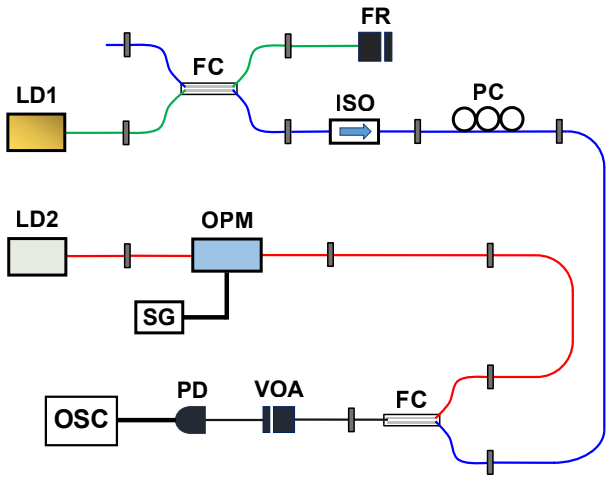

Fig. 1. Experimental setup for bandwidth-enhanced chaos generation. FC: fiber coupler; FR: fiber reflector; ISO: optical isolator; LD1: laser diode 1; LD2: laser diode 2; OPM: optical phase modulator; OSC: real-time oscilloscope; PC: polarization controller; PD: photodiode; SG: signal generator; VOA: variable optical attenuator.

II. EXPERIMENTAL SETUP

The experimental setup for generating bandwidth-enhanced chaos is shown in Fig. 1. In this system, two distributed feedback semiconductor lasers, denoted as laser diode 1 (LD1) and laser diode 2 (LD2), are used to generate chaotic intensity fluctuations and an optical frequency comb, respectively. The injection currents of LD1 and LD2 are both set to approximately six times their threshold current. The temperature of LD1 is stabilized at 25 °C, while the temperature of LD2 is adjusted such that the free-running frequency of LD2 is 40 GHz higher than that of LD1. In addition, LD1 does not include a built-in optical isolator, allowing optical feedback to be applied.

The output of LD1 is directed into an external cavity formed by a fiber coupler (FC) and a fiber reflector (FR), which returns a fraction of the optical field to the laser cavity, driving LD1 into chaotic regime. In this work, the feedback strength P_{f} is defined as the power ratio between the returned feedback light and the free-running output of LD1. Meanwhile, the output of LD2 is passed through an optical phase modulator (OPM), which is driven by a sinusoidal wave with a frequency of f_{m} from an RF signal generator (SG). After phase modulation, an optical frequency comb is generated with evenly spaced comb lines separated by f_{m}.

The chaotic output of LD1 (blue path) and the optical comb (red path) are combined using an additional FC. A polarization controller (PC) is used to ensure proper polarization alignment between the optical fields in the blue and red paths. The combined optical signal is detected by a high-speed photodiode with a 100-GHz 3-dB bandwidth (Fraunhofer HHI). The resulting electrical waveform is directly measured by a 110-GHz real-time oscilloscope (Keysight UXR1104B) for both spectral and temporal analysis. For RBG, the oscilloscope operates as a 10-bit analog-to-digital converter with a sampling rate of 256 GS/s to digitize the electrical waveform. The digitized waveform is then used for entropy rate assessment and RBG.

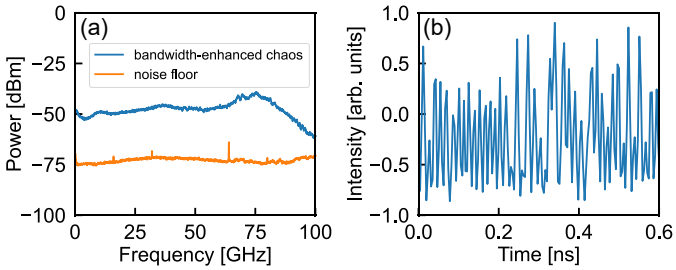

Fig. 2. (a) Electrical spectrum of the bandwidth-enhanced chaos (blue curve) compared with the noise floor (orange curve). The bandwidth-enhanced chaos exhibits a standard bandwidth of 76.8 GHz. (b) Temporal waveform of the bandwidth-enhanced chaos. The fast and random fluctuations make the signal suitable for high-speed RBG.

III. RESULTS AND DISCUSSION

The chaotic output of LD1 is optically combined with the optical frequency comb to generate bandwidth-enhanced chaos. The original chaotic waveform is produced by LD1 under strong optical feedback with $P_{\mathrm{f}} = 0.30$, driving the laser into a high-dimensional chaotic regime. Meanwhile, LD2, after phase modulation at $f_{\mathrm{m}} = 6$ GHz, generates an optical frequency comb with a 6-GHz line spacing. The beat note between the chaotic field and this multi-tone comb extends the overall spectral coverage, thereby enabling the generation of bandwidth-enhanced chaos.

The electrical spectrum of the bandwidth-enhanced chaos exhibits a wide and flat profile, with a standard bandwidth [12] of 76.8 GHz, as shown in Fig. 2(a). Compared with the ∼40 GHz bandwidth reported in leading semiconductor-laser chaos systems [6], [7], the present demonstration achieves nearly twice the previously attainable bandwidth, representing a substantial advancement in chaos bandwidth. The corresponding temporal waveform of the bandwidth-enhanced chaos, shown in Fig. 2(b), exhibits rapid and irregular fluctuations. The highly complex and high-dimensional dynamics of the proposed bandwidth-enhanced chaos make it a high-entropy source suitable for fast RBG.

To quantitatively assess the entropy throughput, the digitized bandwidth-enhanced chaos is analyzed using the NIST SP 800-90B entropy estimation suite [13]. With 10-bit digitization at a sampling rate of 256 GS/s, the estimated minimum entropy is approximately 6.64 bits/sample. This value represents the lowest estimate among seven independent NIST entropy estimators [14], [15] and therefore provides a conservative yet robust measure of the intrinsic randomness of the chaotic source. Notably, the experimentally obtained entropy rate of 1.7 Tbit/s (= 256 GS/s × 6.64 bits/sample) is sufficiently high to support RBG in the Tbit/s regime.

Figure 3 illustrates the procedure used to generate random bits from the digitized bandwidth-enhanced chaos. The

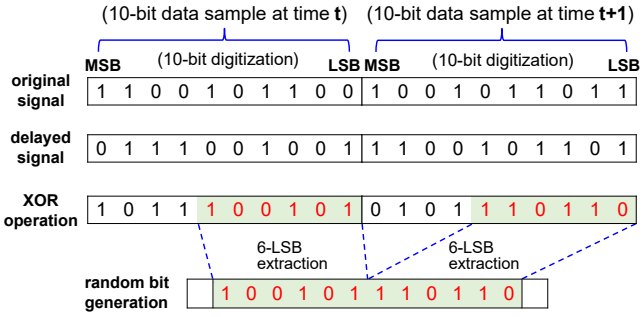

Fig. 3. Procedure for RBG using delayed XOR operation and LSB extraction from the digitized chaos source. MSB: most significant bit; LSB: least significant bit; XOR: exclusive-OR.

chaotic waveform is first sampled and digitized by a 10-bit analog-to-digital converter, producing a sequence of 10-bit data samples. Because physical entropy sources inherently exhibit statistical bias, a simple and widely adopted delayed exclusive-OR (XOR) operation is employed to suppress it [5], [11]. Specifically, the current 10-bit sample is XORed with its 128-sample-delayed counterpart, corresponding to a delay of 0.5 ns. After this bias-removal step, the six least significant bits (LSBs) of the XOR output for each data sample are extracted and concatenated to form a bitstream suitable for high-quality and high-speed RBG.

The resulting 6-LSB bitstream is assessed using the NIST SP 800-22 statistical test suite [5], [6], [11], [16], which comprises 15 tests designed to detect various non-random patterns in the bitstream. In this study, 1000 sequences of 1-Mbit data are collected from the 6-LSB output for statistical assessment. Under a significance level of α = 0.01, a test is considered passed if (i) the P-value (uniformity of p-value) exceeds 0.0001 and (ii) the proportion of 1000 sequences with $p > \alpha$ lies within 0.99 ± 0.0094392. All 15 tests must satisfy these criteria simultaneously to certify statistical randomness.

The results of the NIST SP 800-22 suite, summarized in TABLE I, show that all tests are successfully passed for the 6-LSB bitstream, with both the P-values and the pass proportions well within the acceptable ranges. These results confirm that the bandwidth-enhanced chaos supports an RBG rate of 1.536 Tbit/s (= 256 GS/s × 6 bits) without requiring any complex post-processing, such as high-order differentiation or bit-order-reversal operations. Moreover, the achieved RBG throughput (1.536 Tbit/s) remains safely below the intrinsic entropy rate of the source (1.7 Tbit/s). This consistency verifies that the extracted randomness originates directly from the bandwidth-enhanced chaos, demonstrating true physical RBG.

IV. CONCLUSION

In this work, we experimentally generated bandwidth-enhanced chaos using semiconductor lasers, achieving a standard bandwidth of 76.8 GHz. The intrinsic entropy rate of the source, evaluated using the NIST SP 800-90B suite, reached 1.7 Tbit/s. This level of entropy throughput supports an RBG rate of 1.536 Tbit/s, which is verified by the NIST SP 800-22 suite. Our scheme offers a promising route to realize high-speed photonic random-bit generators for potential applications in secure communication, cryptography, and photonic computing.

TABLE I

NIST SP 800-22 test results for the generated random bitstream. With a significance level of $\alpha = 0.01$ evaluated over 1000 sequences of 1-Mbit data, a test is considered passed if the P-value (uniformity of p-values) exceeds 0.0001 and the pass proportion lies within the interval 0.99 ± 0.0094392 [16]. For tests that yield multiple P-values or pass proportions, the worst-case result is reported [5].

Statistical test	*P*-value	Proportion	Result
Frequency	0.292519	0.9910	Success
Block-Frequency	0.380407	0.9890	Success
Cumulative-Sums	0.091487	0.9880	Success
Runs	0.554420	0.9900	Success
Longest-Run	0.639202	0.9940	Success
Rank	0.781106	0.9880	Success
FFT	0.258307	0.9870	Success
Nonoverlapping Template	0.005762	0.9810	Success
Overlapping Template	0.292519	0.9870	Success
Universal	0.328297	0.9940	Success
Approximate-entropy	0.151190	0.9890	Success
Random Excursions	0.164071	0.9839	Success
Random Excursions Variant	0.080837	0.9823	Success
Serial	0.355364	0.9880	Success
Linear Complexity	0.544254	0.9890	Success

V. ACKNOWLEDGMENT

We would like to express our gratitude to Keysight Technologies in Taiwan for their support in our measurements. This work was supported in part by JSPS KAKENHI (Grant Numbers JP22H05195, JP25H01129, JP25KF0127), JST, CREST (Grant Number JPMJCR24R2), and by the National Science and Technology Council, Taiwan, under Contracts NSTC 114-2112-M-006-004 and 113-2221-E-006-110-MY3.

REFERENCES

[1] K. Yoshimura, J. Muramatsu, P. Davis, T. Harayama, H. Okumura, S. Morikatsu, H. Aida, and A. Uchida, "Secure key distribution using correlated randomness in lasers driven by common random light," *Physical Review Letters*, vol. 108, no. 7, p. 070602, 2012.

[2] H. Gao, A. Wang, L. Wang, Z. Jia, Y. Guo, Z. Gao, L. Yan, Y. Qin, and Y. Wang, "0.75 Gbit/s high-speed classical key distribution with mode-shift keying chaos synchronization of fabry–perot lasers," *Light: Science & Applications*, vol. 10, no. 1, p. 172, 2021.

[3] M. Naruse, T. Matsubara, N. Chauvet, K. Kanno, T. Yang, and A. Uchida, "Generative adversarial network based on chaotic time series," *Scientific Reports*, vol. 9, no. 1, p. 12963, 2019.

[4] H. Miyazawa and M. Fushimi, "An implementation of a 5-term GFSR random number generator for parallel computations," in *Proceedings of the International Symposium on Operations Research and Its Applications (ISORA, 2009)*, 2009, pp. 448–452.

[5] A. Uchida, K. Amano, M. Inoue, K. Hirano, S. Naito, H. Someya, I. Oowada, T. Kurashige, M. Shiki, S. Yoshimori *et al.*, "Fast physical random bit generation with chaotic semiconductor lasers," *Nature Photonics*, vol. 2, no. 12, pp. 728–732, 2008.

[6] R. Sakuraba, K. Iwakawa, K. Kanno, and A. Uchida, "Tb/s physical random bit generation with bandwidth-enhanced chaos in three-cascaded semiconductor lasers," *Optics Express*, vol. 23, no. 2, pp. 1470–1490, 2015.

[7] Q. Zhang, L. Jiang, J. Sun, Y. Pan, J. Feng, A. Yi, W. Pan, B. Xu, and L. Yan, "Multi-channel broadband optical chaos generation assisted by phase modulation and CFBG feedback," *Optics Express*, vol. 32, no. 12, pp. 20 471–20 482, 2024.

[8] Y. Han, S. Xiang, Y. Wang, Y. Ma, B. Wang, A. Wen, and Y. Hao, "Generation of multi-channel chaotic signals with time delay signature concealment and ultrafast photonic decision making based on a globally-coupled semiconductor laser network," *Photonics Research*, vol. 8, no. 11, pp. 1792–1799, 2020.

[9] J. D. Hart, Y. Terashima, A. Uchida, G. B. Baumgartner, T. E. Murphy, and R. Roy, "Recommendations and illustrations for the evaluation of photonic random number generators," *APL Photonics*, vol. 2, no. 9, 2017.

[10] N. Li, B. Kim, V. Chizhevsky, A. Locquet, M. Bloch, D. Citrin, and W. Pan, "Two approaches for ultrafast random bit generation based on the chaotic dynamics of a semiconductor laser," *Optics Express*, vol. 22, no. 6, pp. 6634–6646, 2014.

[11] 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," *Optics Express*, vol. 18, no. 6, pp. 5512–5524, 2010.

[12] F.-Y. Lin, Y.-K. Chao, and T.-C. Wu, "Effective bandwidths of broadband chaotic signals," *IEEE Journal of Quantum Electronics*, vol. 48, no. 8, pp. 1010–1014, 2012.

[13] M. S. Turan, E. B. Barker, J. M. Kelsey, K. A. McKay, M. L. Baish, and M. Boyle, "Recommendation for the entropy sources used for random bit generation," National Institute of Standards and Technology, Special Publication 800-90B, 2018.

[14] C.-H. Tseng, R. Funabashi, K. Kanno, A. Uchida, C.-C. Wei, and S.-K. Hwang, "High-entropy chaos generation using semiconductor lasers subject to intensity-modulated optical injection for certified physical random number generation," *Optics Letters*, vol. 46, no. 14, pp. 3384–3387, 2021.

[15] C.-H. Tseng, R. Funabashi, K. Kanno, A. Uchida, C.-C. Wei, and S.-K. Hwang, "Entropy analysis on chaos excited through destabilization of semiconductor lasers at period-one nonlinear dynamics for physical random number generation," *Optics Express*, vol. 32, no. 13, pp. 23 097–23 114, 2024.

[16] A. Rukhin *et al.*, "A statistical test suite for random and pseudorandom number generators for cryptographic applications," National Institute of Standards and Technology, Special Publication 800-22 Revision 1a, 2010.