Novel Optical Fast Random Number Generators Based on Integer Domain Chaotic Iterations

Qianxue Wang[1], **Simin Yu**[1], **and Xiaole Fang**[2]

[1]College of Automation, Guangdong University of Technology, China
[2]Land and Resources Technology Center of Guangdong Province, China

Abstract— For cryptography and secure communications, it is very prerequisite that the random number generator (RNG) is based on non-deterministic physical mechanisms, extremely fast generator and robustness to noise are required. In this work, we present novel fast optoelectronic architecture RNGs based on integer domain chaotic iteration (IDCI), with a chaotic semiconductor laser, having time-delayed self-feedback. The solution stems from some well-defined discrete chaotic iterations that satisfy the reputed Devaney's definition of chaos, namely the integer domain chaotic iterations technique, improve the statistical properties of this RNG. Using standard criteria named NIST and DieHARD (famous batteries of tests), the randomness of the output sequences is verified.

1. INTRODUCTION

Due to the rapid development of the Internet in recent years, the discovery of fast random number generator (RNG) with a strong level of security is thus becoming a hot topic, because numerous cryptosystems and data hiding schemes are directly dependent on the quality of these generators. Considerable improvements for the rate of chaotic random bits generator have been however reached by using a semi-conductor laser in the presence of external feedback [11], a well known setup in chaotic optical systems.

However, according to the analysis of [7], correct sampling method and using Most Significant Bits (MSB) is a key factor to preserve the deterministic origin in the generator of random streams using optoelectronic chaotic lasers. However if the sequence keeps the most large part of information on the signal, its statistical performance might be not good. Integer domain chaotic iteration has been proved not only to assign discrete chaotic properties to the output streams (if the input source is truly unpredictable random), but also to improve the statistical properties of various defectives PRNGs [2]. Thus we think interesting to regard weather this approach can work too for chaotic laser based pseudorandom generator.

In this paper, the study of using broadband optical signal to generate random binary sequence according to the method proposed in [7], is going to be deepen. We propose to apply the same method on the chaotic waveform generated by broadband photonic oscillations with or without integer domain chaotic iterations, and to analyze the differences.

2. SETUP FOR THE CHAOTIC LASER

Indeed, as shown in Fig. 1, the chaotic laser signal considered in this paper is similar to the one described in [7], except that there is no output signal for photonic noise. This physical source of entropy presents a very strong determinism. The output chaos signal is generated by a nonlinear dual delay differential equation implemented in an optoelectronic and electro-optic feedback loop.

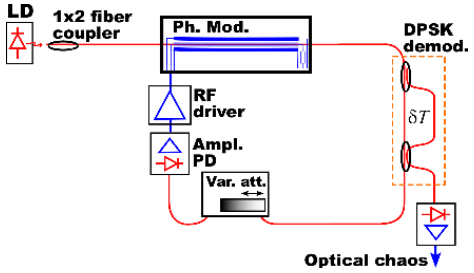


Figure 1: Chaotic laser signal setup.

3. XOR IDCI

In this section, we first introduce the basic concept of IDCI. Let $N \in \{1, 2, \ldots\}$ be a positive integer, $\mathbb{B} = \{1, 0\}$ denotes the set of binary numbers, while $\mathbb{B}^N$ is the set of binary vectors of size N. The integer $x^n \in \{0, 1, 2, \ldots, 2^N - 1\}$, $n = 0, 1, 2, \ldots$ is represented using N bits in base-2: $x^0 = (x^0_{N-1} x^0_{N-2} \ldots x^0_0) \in \mathbb{B}^N$ is the initial condition, while $x^{n-1} = (x^{n-1}_{N-1} x^{n-1}_{N-2} \ldots x^{n-1}_0) \in \mathbb{B}^N$ and $x^n = (x^n_{N-1} x^n_{N-2} \ldots x^n_0) \in \mathbb{B}^N$ denote the $n-1$-th and n-th iteration respectively. In IDCI systems, the iterative equation is defined as follows:

$$x^n_i = \begin{cases} x^{n-1}_i & \text{if} \quad i \neq s^n \\ (f(x^{n-1}))_i & \text{if} \quad i = s^n, \end{cases} \tag{1}$$

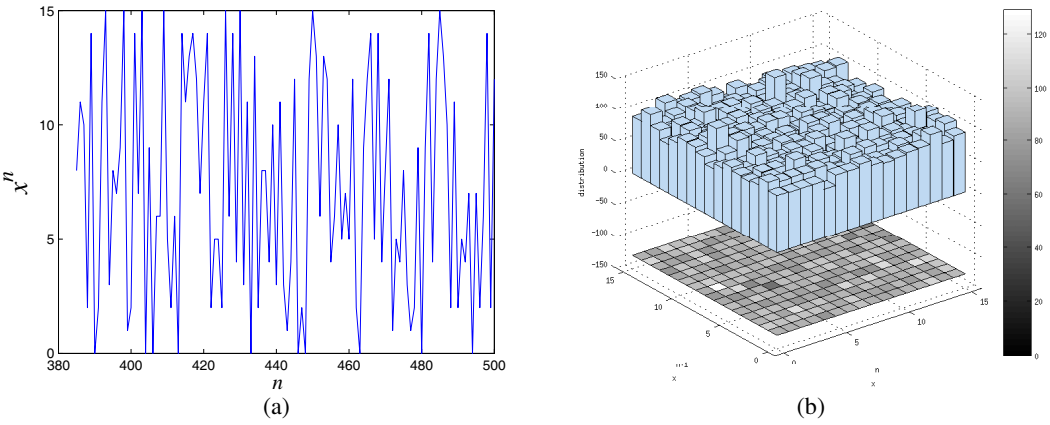
where $i = 0, 1, 2, \ldots, N-1$, $n = 1, 2, \ldots$, and $s = (s^1 s^2 \ldots s^n \ldots)$ is an one-sided infinite sequence of integers bounded by $N-1$: $\forall n \in \mathbb{N}^*$, $s^n \in \{0, 1, 2, \ldots, N-1\}$. Additionally, the iterate function f is usually the vectorial Boolean negation, given by $f(x^{n-1}) = (\overline{x^{n-1}_{N-1}}\, \overline{x^{n-1}_{N-2}} \ldots \overline{x^{n-1}_i} \ldots \overline{x^{n-1}_0})$, and the following notation is used: $(f(x^{n-1}))_{i=s^n} = (\overline{x^{n-1}_{N-1}}\, \overline{x^{n-1}_{N-2}} \ldots \overline{x^{n-1}_i} \ldots \overline{x^{n-1}_0})_{i=s^n} = \overline{x^{n-1}_{i=s^n}}$, that is, $(f(x^{n-1}))_{i=s^n}$ is the i-th component of $f(x^{n-1})$. Let us finally remark that, in IDCI, the one-sided infinite sequence of integers $s = (s^1 s^2 \ldots s^n \ldots)$ is usually named a chaotic strategy.

Secondly, XOR IDCI is one of the IDCIs, instead of updating only one component at each iteration a subset of components are updated together, which is introduced in [1]. Comparing with the other IDCIs, XOR IDCI is much more compatible in physical design. Here the updating function is chosen as the vectorial negation, the iterative equation can be rewritten as:

$$x^n = x^{n-1} \oplus s^n \tag{2}$$

where x^n and x^{n-1} are integers, which are represented in binary form as $x^n = (x^n_{N-1} x^n_{N-2} \ldots x^n_0) \in \mathbb{B}^N$ and $x^{n-1} = (x^{n-1}_{N-1} x^{n-1}_{N-2} \ldots x^{n-1}_0) \in \mathbb{B}^N$ and $s = (s^1 s^2 \ldots s^n \ldots)$ is an one-sided infinite sequence of integers bounded by $N-1$: $\forall n \in \mathbb{N}^*$, $s^n \in \{0, 1, 2, \ldots, N-1\}$.

Select $N = 4$, chaotic waveforms obtained by simulation as shown in Fig. 2(a). Fig. 2(b) shows the intensity map for $N = 4$. In order to appear random, the histogram should be uniformly distributed in all areas. It can be observed that a uniform histogram and a flat color intensity map are obtained when using XOR IDCI.



(a) (b)

Figure 2: Chaotic waveforms and histogram of XOR IDCI for $N = 4$. (a) Chaotic waveforms. (b) Histogram.

The single basic component presented in Equation (2) is of ordinary use as a good elementary brick in various PRNGs, it corresponds to the discrete dynamical system in chaotic iterations.

4. RNG APPROACHES BY APPLYING IDCI METHOD TO CHAOTIC LASER

4.1. Devaney's Chaos Property

Generally speaking, the quality of a RNG depends, to a large extent, on the following criteria: randomness, uniformity, independence, storage efficiency. A chaotic sequence may satisfy these requirements and also other chaotic properties, as ergodicity, entropy, and expansivity. A chaotic

sequence is extremely sensitive to the initial conditions. That is, even a minute difference in the initial state of the system can lead to enormous differences in the final state, even over fairly small timescales. Therefore, chaotic sequence fits the requirements of (or pseudo-)random sequence well. However, despite a large number of papers published in the field of chaos-based generators, the impact of this research is rather marginal. This is due to the following reasons: almost all PRNG/RNG algorithms using chaos are based on dynamical systems defined on continuous sets (e.g., the set of real numbers). So these generators are usually slow, requiring considerably more storage space, and lose their chaotic properties during computations as mentioned earlier in this paper. These major problems restrict their use as generators [8]. For RNG approaches by applying IDCI method to chaotic laser, we do not simply integrate chaotic maps hoping that the implemented algorithm remains chaotic. Indeed, the IDCI method we used here is just discrete chaotic iterations and have been proven in [1] that these iterations produce a topological chaos as defined by Devaney: they are regular, transitive, and sensitive to initial conditions. This famous definition of a chaotic behavior for a dynamical system implies unpredictability, mixture, sensitivity, and uniform repartition. Moreover, as only integers are manipulated in discrete chaotic iterations, the chaotic behavior of the system is preserved during computations, and these computations are fast. For the approaches listed in this section, XOR IDCI method is applied because of its easy adoptable algorithm.

4.2. Approach 1: Improve the Performance of Randomness via IDCI

To improve the optical RNGs, as shown in Fig. 3. XOR IDCI is used.

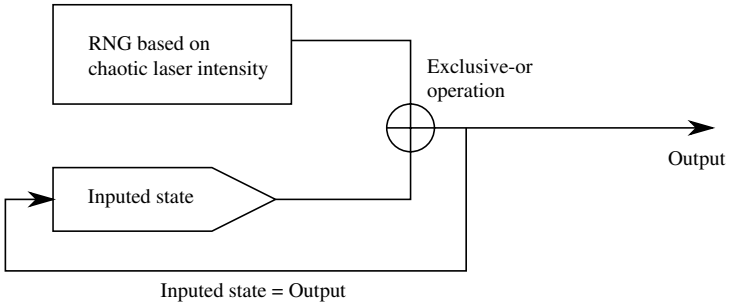


Figure 3: The XOR IDCI scheme applied to optical RNG.

Here, RNG introduced in [3, 4] is used to demonstrated. Firstly, our chaotic laser intensity is undersampled at rate clock 2.5 GHz; Then three times difference of nearest neighbor points (in [3, 4], it is named "derivative") are computed for all obtained values; At last, the 8 LSBs of each difference value are collected to build as a random sequence. To apply the XOR IDCI, the initial state will be randomly set as an 8-bits value, every 8 LSBs built out from the generator are then exclusive-or with the state value as Fig. 3, its output is appended as random sequence and also feedback as new state value.

For verifying the improvement of XOR IDCI, the output sequence (10^8 bits) with and without XOR IDCI are tested by NIST and DieHARD battery suite, which are famous statistical standard tests for RNGs [6, 9]. After XOR IDCI merged, the NIST suite are successfully passed all, and passing rate of DieHARD suite are improved from 11/18 to 15/18.

4.3. Approach 2: Chaotic Laser Sample Data with Multiple IDCI

In this section, firstly, the RNG with IDCI methods stratifies the Devaney's chaos property, a brief description is given; Then the method that XOR IDCI used to improve the RNGs based on chaotic laser is introduced; At last a new scheme based on XOR IDCI to generate random numbers with chaotic laser intensity is depicted, which is able to reach 320 GHz generator speed and very good robustness to external perturbations.

Table 1: The passing rate for different n of IDCIORNG in NIST and DieHARD tests.

Tests \ n	1	10	20	30	40
NIST suite	0/15	14/15	15/15	15/15	15/15
DieHARD suite	1/18	11/18	14/18	18/18	18/18

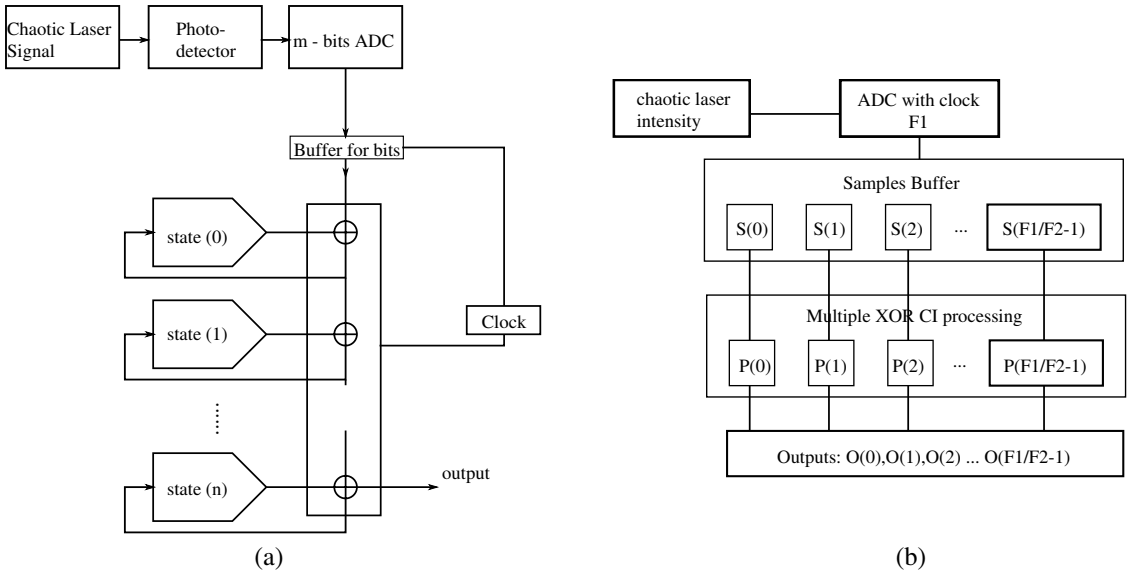


Figure 4: Experimental setup of the optical system used to generated signal as physical random sources for random bit sequences. (a) Multiple XOR IDCI. (b) Parallel processing to IDCIRNG.

For achieve good randomness, a multiple mode of XOR IDCI is used, as shown in Fig. 4(a), n state values and XOR IDCI iteration have been used, every state value will be randomly initialed as an m-bits integer for respective to the buffer. In our experiments, the chaos laser intensity are undersampled at 8-bit 40 GHz rate, and initial state are set as 8-bit, hence the undersampling frequency 40 GHz $\times$ 8 bits = 320 Gbitps is achieved. Here we named such generator IDCIORNG (chaotic iteration optical random number generator).

To test the randomness of the IDCIORNG, 10^8 bits output sequence are tested by NIST and DieHARD test suite, $n = 1, 10, 20, 30$, and 40 are used for IDCIORNG in tests to make a comparison. The passing rates of the test results are shown in Table 1, it is not difficult to find out increasing the n, the XOR IDCI processing, can improve the statistical performance. When $n \geq 30$, all test suited are able to be successfully passed.

4.4. Approach 3: Parallel Processing to IDCIRNG Based on Chaotic Laser

In Approach 2, random stream generator might be related to two elements: Firstly, in 40 GHz sampling frequency, the correlations between neighbor sampled values are very small; Secondly, the chaotic iterations are rearranging the distribution of the sample values. If we increase the sampling frequency, the correlation between two adjacent samples are correspondingly increased, and that leads random number generator impossible. To solving this problem, a parallel architecture would be applied.

Firstly assuming that the chaotic laser signal with bandwidth F_0 has been sampled by very huge frequency F_1, which $F_1 \gg 2 \times F_0$, that means such sample are designed to follow the classical Shannon sampling theorem (The Shannon sampling theorem indeed states that a limited bandwidth signal can be digitized without loss of information, when the sampling frequency is at least twice the maximum signal frequency); Secondly, frequency F_2 is known to be small enough to break the correlations between nearest samples, we divided the samples into F_1/F_2 parts and F_1/F_2 multiple XOR IDCI processes are prepared, the first F_1/F_2 samples are arranged as $S_0, S_1, S_2, \ldots, S_{(F_1/F_2)-1}$ then put into their corresponding processes, then $S_{F_1/F_2}, S_{(F_1/F_2)+1}, \ldots, S_{2(F_1/F_2)-1}$ for the second ones and so on; At last, the output from the processes are collected as random sequence. The procedure is shown in Fig. 4(b), the speed of such generator is extremely fast, we define in ADC we use n-bit sampling length, then the produce rate can reach $n/timeF_1$ in theory.

The standard statistical tests: NIST and DieHARD suites are applied here to verify the approach 3. An chaotic laser signal data are stimulated in computer with the method from [5], its frequency is $F_1 = 4000$ GHz, and corresponding parameters is listed as:

- **Time delay**: Set as 60 ns;
- **High Frequency Cut-off**: 13 ps;
- **Ratio between high and low frequency cut-off**: 5×10^{-5};

- **Type of nonlinear transformation**: square of Sine;
- **Highest complexity chaotic regime**: 5.

Here the states in XOR IDCI processing are set as 32-bits words, which are generated from XOR-shift, which are designed by George Marsaglia [10], and each process provide 30 times iterations. Then three random sequence are generated by:

- **Sequence1**: By approach 2, every data are quantized by 8-bits, it can achieve $8 \times 4000 = 3.2/times10^4$ GHz;
- **Sequence2**: By approach 3, every data are quantized by 8-bits, $F_2 = 40$ GHz, then there are $4000/40 = 100$ XOR IDCI processes, it can achieve $8 \times 4000 = 3.2 \times 10^4$ GHz;
- **Sequence3**: By approach 3, every data are quantized by 1-bits, $F_2 = 40$ GHz, it can achieve 4000 GHz.

And the passing rate of the tests are shown in Table 2, Sequence1 generated by approach 2 are really bad in randomness as we predict. For NIST, the Sequence2 and Sequence3 are both fluently pass them all, but for DieHARD, Sequence2 is able to pass, and Sequence 3 fail 3 subjects.

Table 2: The passing rate of NIST and DieHARD.

Sequence / **Tests**	Sequence1	Sequence2	Sequence3
NIST suite	1/15	15/15	15/15
DieHARD suite	3/18	18/18	15/18

5. CONCLUSION

Three examples of mixing IDCI and MSB of optoelectronic chaotic signal are given, the results of NIST and DieHARD test suite show the improvements of randomness, in future, the practical implementation is looking forwarded.

ACKNOWLEDGMENT

This work was supported by the National Natural Science Foundation of China under Grant 61172023; by the Specialized Research Foundation of Doctoral Subjects of Chinese Education Ministry under Grant 20114420110003; and by China Postdoctoral Science Foundation No. 2014M552175.

REFERENCES

1. Bahi, J., R. Couturier, C. Guyeux, and P.-C. Héam, "Efficient and cryptographically secure generation of chaotic pseudorandom numbers on gpu," *CoRR*, abs/1112.5239, 2011.
2. Bahi, J., X. L. Fang, C. Guyeux, and Q. X. Wang, "Suitability of chaotic iterations schemes using xorshift for security applications," *Journal of Network and Computer Applications*, Vol. 37, 282–292, 2014.
3. Kanter I., et al., "An optical ultrafast random bit generator," *Nature Photonics*, Vol. 4, No. 1, 58–61, 2010.
4. Reidler, I., et al., "Ultrahigh-speed random nuber generation based on a chaotic semiconductor laser," *Physical Review Letters*, Vol. 103, No. 2, 24–28, Jul. 2009.
5. Michael, P., et al., "Routes to chaos and multiple time scale dynamics in broadband bandpass nonlinear delay electro-optic oscillators," *Phys. Rev. E*, Vol. 79, 026208, Feb. 2009.
6. Andrew, R., et al., "A statistical test suite for random and pseudorandom number generators for cryptographic applications," 2001.
7. Fang, X. L., et al., "Noise and chaos contributions in fast random bit sequence generated from broadband optoelectronic entropy sources," *IEEE Trans. Circ. Syst. I*, Vol. 61, No. 3, 888–901, Mar. 2014.
8. Kocarev, L., "Chaos-based cryptography: A brief overview," *IEEE Trans. Circ. Syst. Mag.*, Vol. 7, 6–21, 2001.
9. Marsaglia, G., "Diehard battery of tests of randomness," Florida State University, 1995.
10. Marsaglia, G., "Xorshift rngs," *Journal of Statistical Software*, Vol. 8, No. 14, 1–6, 2003.
11. Mukai, T. and K. Otsuka, "New route to optical chaos: Successive-subharmonic-oscil-lation cascade in a semiconductor laser coupled to an external cavity," *Physical Review Letters*, Vol. 55, No. 17, 17–11, 1985.