New alternate ring-coupled map for multi-random number generation

Andrea Espinel Rojas, Ina Taralova, René Lozi

NEW ALTERNATE RING-COUPLED MAP FOR MULTI-RANDOM NUMBER GENERATION

Andrea Espinel, Ina Taralova and René Lozi *†‡

Abstract. An improved Lozi function with alternate coefficients has been proposed. The modifications in the model allow to remove the holes in the attractor which are not desirable, but appeared in the previous Lozi function; in this way, an everywhere dense attractor can be obtained. Moreover, the strong sensitivity to the type of binarisation (conversion of real values to 0 and 1) has been demonstrated; this conversion to binary numbers is instrumental to apply the NIST tests for randomness. The results have been validated and compared via NIST tests, for the different methods of quantization. Finally, is has been verified that the multi-random properties of the output signal have been improved thanks to the following strategies : under-sampling of the output signal, and the system order increasing.

Keywords. Nonlinear dynamical system, ring-coupled map, Lozi function, NIST tests, discrete-time map, dense chaotic attractor, pseudo random number generator

1 Introduction

The accelerated development of modern data transaction applications such as telecommunications requires encoding techniques with higher standards of security. Classically, these encoding sequences are obtained using Pseudo Random Number Generators (PRNG). As an efficient alternative, the chaotic-based generators are used to achieve even higher demanding encryption standards. Indeed, the chaotic systems exhibit a plethora of properties which make them suitable to meet the above requirements. The advantage to use chaotic systems lies in their extreme sensitivity to small parameter and initial conditions variations: in this way, as many different chaotic carriers as wanted can be generated.

However, the appropriate selection of a chaotic map that satisfies cryptographic applications requirements is a huge problem. It has to be emphasized that all chaotic maps are not applicable, because the chaotic generator - which is deterministic - has to satisfy at the same time the criteria for closeness to random signals. Therefore many practical problems arise, from the choice of the chaotic generator and its parameters, to the chaotic properties verification after the quantisation. Ideally, for cryptographic applications and higher security, an everywhere dense chaotic attractor is required, so all chaotic signal samples shall appear with the same probability (indeed, if there are holes in the chaotic attractor, the values of the state vector corresponding to the holes will never take place).

Other emerging applications in environmental sciences (global warming) or biology (multi-agent competition) require also a plethora of mutually independent random sequences (i.e. multi-random numbers). Unfortunately, most of the existing random number generators are virtually unable to meet these requirements: the correlation between the generated sequences by a classical PNRG increases with the number of sequences [12]. The authors in [10] analyze popular PRNGs working in parallel (e.g. the 32-bit generator `rand`, the combined multiple-recursive generator, and the additive lagged-Fibonacci generator), and demonstrate the lack of independence of the generated streams.

For the classical PNRG satisfying such requirements there are others issue: as an example the famous Blum Blum Shub generator (BBS) is cryp-

*Andrea Espinel and Ina Taralova are with L'UNAM, IRCCyN, École Centrale de Nantes, France. E-mails: andrea.espinel-rojas, ina.taralova@irccyn.ec-nantes.fr

†René Lozi is with Laboratoire J.A. Dieudonné, UMR CNRS 7351, Université de Nice Sophia-Antipolis, France. E-mail:lozi@unice.fr

‡Manuscript received; revised

tographically safe provided the use of a really big modulus M (with tens or even hundred of digits) and it is excruciatingly slow. Some estimates give the producing of one million random bits would take about 5 minutes, in comparison our alternate ring-coupled map allows the production of hundreds of million random bits per second, i.e., more than 10,000 times faster.

Moreover BBS needs special programming using integer operation working on hundred of digits, instead of using the very fast FPU, implemented in up to date microprocessors.

Lozi had demonstrated that highly efficient discrete-time chaotic generators can be obtained from quite simple models such as the piece-wise linear ones, under some conditions [7, 8]. Therefore, the aim of our work is to develop a new alternate Lozi function, which guarantees the statistical independence of the state variables. This objective can appear contradictory at a first glance, since the deterministic modelling implies a coupling between the sate variables. However, it will be shown that a particular ring-coupling, already studied in [3], enhances the nice chaotic properties, and improves the statistical features. To evaluate the random properties of these generators, a set of statistical based test known as NIST test developed by the National Institute of Standards and Technology are to be used [11].

2 System Definition

A first coupled chaotic map confined to the 2D torus has already been proposed as a PRNG in [1], which random characteristics have been validated using the NIST tests. This coupling has been imposed because the one-dimensional chaotic map exhibits numerical instability (convergence to the unstable fixed point -1 instead of the chaotic attractors) [5]. Moreover, the coupling parameter improved the statistical properties of the resulting system. The particularity of the coupling here is that each state variable x^j is coupled only with itself and x^{j+1}, see Figure 1. At first glance, it could seem interesting to add supplementary cross couplings between the state variables, as shown in Figure 2, in order to enrich the random properties of the map. However, in this case a cross-coupling is inappropriate because it would increase the determinism and therefore deteriorate the statistical properties which we are looking for.

In the previous study [1], the state variables were not equidistributed: it has been demonstrated that the chaotic attractor exhibited holes delimited by the discontinuity lines and their forward iterates. Therefore, there have been regions in the state space which the system orbits never visited, thus deteriorating the randomness.

To improve the latter results, in this paper we deal with the new Lozi system with alternate coupled maps, confined to the p-dimensional torus $T^p = [-1, 1]^p$ by the map $M_p : T^p \Rightarrow T^p$

$$M_p : \begin{aligned} x^1_{n+1} &= 1 - 2\left|x^1_n\right| + k^1 \times x^2_n \\ x^2_{n+1} &= 1 - 2\left|x^2_n\right| + k^2 \times x^3_n \\ &\vdots \\ x^p_{n+1} &= 1 - 2\left|x^p_n\right| + k^p \times x^1_n \end{aligned} \tag{1}$$

where the parameters $k^i = (-1)^{i+1}$. A previous model with non alternate coefficients has been proposed in [1], with $k^i = 1$. As the trajectories of the map are unbounded, the state variables are contained on the torus:

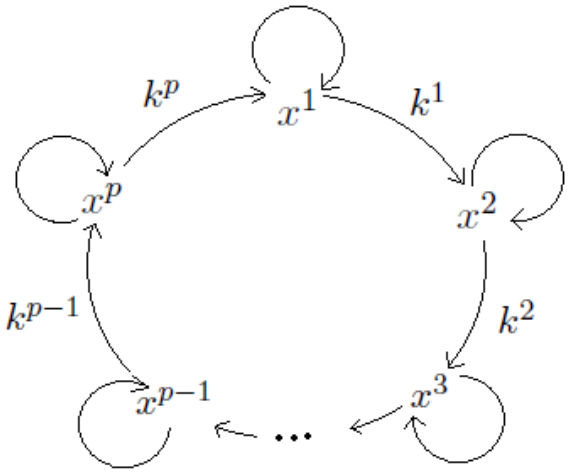

Figure 1: Ring-coupling between the state variables

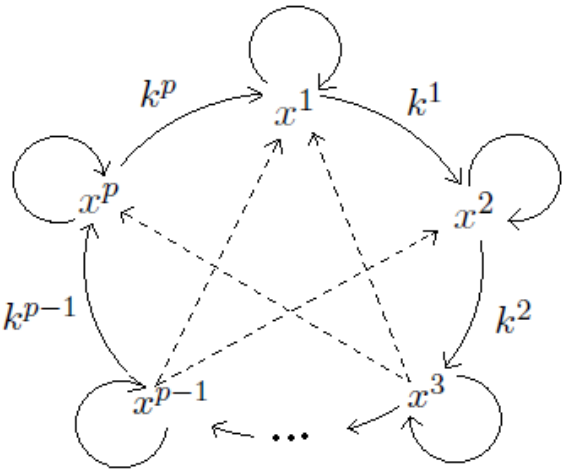

Figure 2: Cross coupling between the state variables

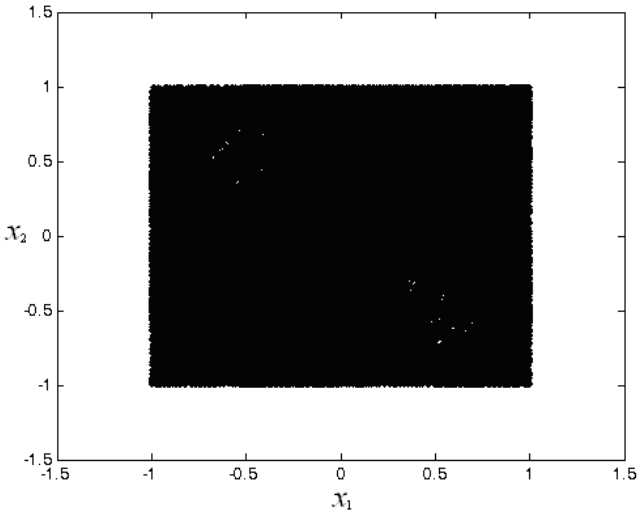

Figure 3: Map M_2 (2) on the torus $T^2 = [-1, 1]^2$

$$
\begin{aligned}
&if\ x_{n+1}^j = 1 - 2\left|x_n^j\right| + k^j \times x_n^{j+1} < -1 \\
&\qquad add\ 2 \\
&if\ x_{n+1}^j = 1 - 2\left|x_n^j\right| + k^j \times x_n^{j+1} > 1 \\
&\qquad substract\ 2
\end{aligned}
\tag{2}
$$

where $|x_n|$ denotes the absolute value of x_n, and $j \in [1, p]$. The alternate sign modification proposed in this paper eliminates the holes from the previous model (with only positive signs), and therefore the resulting basin of attraction is everywhere dense, which is very satisfactory for the RNG applications, see Figure 3. (The transient of 10.000 points has been cut off).

In addition, notice that this 2-dimensional chaotic attractor (which is a torus: $A \equiv B \equiv C \equiv D$ are the same point) coincides exactly with the four symmetrical regions of the phase plane, defined by the function $|x_n|$, see figure 4. In this figure, an example of trajectory is also shown for better understanding of the containment process. For $x_n^1 = 0.2587$, $x_n^2 = 0.7876$, the value of x_{n+1}^1 before confinement (represented by x_{n+1}^j) falls outside the 2-dimensional torus T^2: $x_{n+1}^j = 1.2702$, making the trajectory diverge after a few iterations. To guarantee that the trajectory remains bounded, the state x_{n+1}^j is pushed back into the attactor, by substracting 2: $x_{n+1}^1 = -0.7298$. As $x_{n+1}^2 = -0.8339$ stays into the torus, the state keep this value. However, in the case that x_{n+1}^2 leaves the square $[-1, 1]^2$, it should also be confined into the torus.

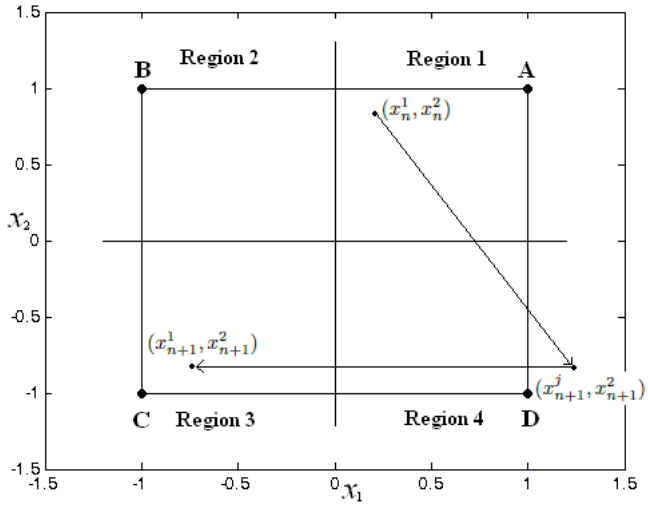

Figure 4: 2-dimensional chaotic attractor: $T^2 = [-1, 1]^2$

3 Results and Discussion

The random properties validation of a 4- dimensional system have been validated using the NIST Test Suite. This consists of 15 different tests that evaluate the randomness of binary sequences generated by RNG and PRNG. The purpose of each test is to verify the consistence of the following conditions with the values that would be expected from a truly random sequence, see Table 1. Each tests validate by default a sequence as being random (called the null hypothesis H0), and the idea is to show that there is no enough evidence to reject this proposition. Here, as the chaotic carrier output

generated by the map (2) for each iteration n is a real value, it needs to be binarized, in order to be eligible for validation as being random using the package of NIST Test [11]. In other words, each value of the sequence has to be represented in terms of binary digits: 1 (one) or 0 (zero) to be evaluated.

For our application, different methods of binarisation (converting real signals to binary ones) have been implemented and compared. A first 1-bit binarisation has been applied to the system (2) output defined as $y_n = x_n^k$, with k chosen in $[1, p]$:

$$\begin{aligned} &if\ y_n \geq 0 && b = 1 \\ &else && b = 0 \end{aligned} \tag{3}$$

The results for the 4-dimentional system have shown to be highly sensitive to the type of binarisation. Standart single (32 bits) and double (64 bits) precision types of binarisation as the IEEE754 form [4] have been compared. Since the system is confined to the p-dimensional torus $T^p = [-1, 1]^p$, all significant figures of the output value belong to the decimal part of the number. In other words, for every chaotic career the real part is always zero, so a binary representation of this part of the figure is no necessary. It is also important not to exceed the number of bits representing the decimal part. This will cause repeated subsequences inside the entire sequence, generating a loss of randomness. Therefore, after testing different methods, a 32-bit binarisation has been chosen as being the most suitable solution: 31 bits are assigned to represent the decimal part (being b_0 the less significant bit, and b_{30} the most) , and 1 bit to the sign (b_{31}). For example, if $y_n = 0.6835$, then the corresponding binary sequence to this value is:

$$\underset{b_{31}}{|\,0\,|}\ \underset{b_{30}}{1010111011111001110110110010001|}\ \xleftarrow{\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad} \underset{b_0}{}$$

Using MATLAB R2009a toolbox [9]:

$$q = quantizer\left([32, 31]\right)$$

$$b = num2bin\left(q, y_n\right)$$

To illustrate the results, the NIST test using a binary input for the four dimensional Lozi system M_4 (2) with parameters $\left[k^1, k^3\right] = 1$, $\left[k^2, k^4\right] = -1$ are shown in Table 2 for a 1-bit binarisation, and for the 32-bit most appropriate binarisation technique in Table 3. For comparison, the same conditions as in [1] have been chosen:

Length of the original sequence: 10^8 bits
Length of *bit string*: 1M
Quantity of *bit strings*: 100

The output of the system has been arbitrary chosen as being: $y = x^4$.

P-VALUE		PROPORTION		STATISTICAL TEST
0.935716		99/100		Frequency
0.000000	*	100/100		BlockFrequency
0.987896		99/100		CumulativeSums
0.153763		100/100		Runs
0.153763		100/100		LongestRun
0.816537		100/100		Rank
0.699313		99/100		FFT
0.000000	*	95/100	*	NonOverlappingTemplate
0.030806		98/100		OverlappingTemplate
0.657933		99/100		Universal
0.000000	*	3/100	*	ApproximateEntropy
0.804337		61/62		RandomExcursions
0.500934		59/62		RandomExcursionsVariant
0.000000	*	92/100	*	Serial
0.739918		97/100		LinearComplexity

Table 2: NIST test for the 4^{th} order Lozi function (2) and 1-bit binarisation, eq.(3)

P-VALUE	PROPORTION	STATISTICAL TEST
0.419021	100/100	Frequency
0.213309	100/100	BlockFrequency
0.978072	99/100	CumulativeSums
0.075719	100/100	Runs
0.867692	99/100	LongestRun
0.494392	99/100	Rank
0.334538	99/100	FFT
0.213309	99/100	NonOverlappingTemplate
0.616305	99/100	OverlappingTemplate
0.779188	100/100	Universal
0.474986	99/100	ApproximateEntropy
0.452799	68/69	RandomExcursions
0.063482	69/69	RandomExcursionsVariant
0.437274	98/100	Serial
0.739918	99/100	LinearComplexity

Table 3: NIST test for the 4^{th} order Lozi function (2) and 32-bit binarisation

Furthermore, as the results show their independence from the initial conditions, every *bit string* in this first test is the resulting sequence of a different

TEST	**CONDITION**
The Frequency (Monobit) Test	Quantity of ones and zeros in a sequence
Frequency Test within a Block	Frequency of ones in a sub-sequence or block
The Runs Test	Total uninterrupted sequences of identical bits (runs)
Tests for the Longest-Run-of-Ones in a Block	Longest run of ones in a subsequence
The Binary Matrix Rank	Test Linear dependence between sub-sequences
The Discrete Fourier Transform (Spectral) Test	Periodic patterns in the sequence
The Non-overlapping Template Matching Test	Occurrence of a non-periodic target string or template
The Overlapping Template Matching Test	Occurrence of a specific template of ones
Maurer's Universal Statistical Test	Possibility to compress the sequence without loosing information
The Linear Complexity Test	Linear complexity of the sequence
The Serial Test	Occurrence of all possible overlapping m-bit patterns
The Approximate Entropy Test	As The Serial Test, but comparing patterns of m and m+1 lengths
The Cumulative Sums (Cusums) Test	Length of the cumulative sum of partial sequences or random walk
The Random Excursions Test	Number of visits of a random walk to a certain state or integer value
The Random Excursions Variant Test	Number of visits to various states in a random walk

Table 1: General description of the 15 different NIST Tests

randomly chosen initial condition.

There are two different criterions to interpret and evaluate the results. For the first one, the principle for a successful test is that a quantifier called p-value has to be superior to the significance level (0.01 for this case). This quantifier evaluates the uniformity of the zeros and the ones distribution in the sequence.

The second approach examines the proportion of sequences passing the current statistical test. In this particular case, the minimum pass rate is around 96 for a simple size of 100 binary sequences for the group of statistical test excepting the random excursion (variant) tests, which minimum pass rate always changes. For example, for a sample of 63 binary sequences, the minimum pass rate is approximately 60. However, the non-success of a determinate test is always represented by an asterisk (*) in the table report. For the present model (2), all tests have been successful thus the sequence can be accepted as being random. Thus, the results demonstrate that the new system has better statistical performances than the initial system without alternate coefficients presented in [1].

There are some procedures that improve the random properties of the signal, making the sequence properties less sensitive to the different binarization methods. Here, two possible strategies are suggested: undersampling of the output signal, or increasing the system order.

Different under-samplings have been tested from which the "1 out of 10" showed to be particularly successful. The "1 out of 10" under-sampling strategy results are shown in Table 4, for a 1-bit binarisation. The conditions for the NIST test are identical to the NIST test for the 4-dimentional Lozi system. Here, it is shown that even using the poorest binarization method for evaluation, the sequence passes all NIST tests successfully.

For the second method, the random properties validation of a 10-dimensional system has been carried out and the results are shown in Table 5. The conditions and binarisation (1-bit method) are the same as in the previous procedure. In addition, the initial

condition has been randomly chosen:

$$x_0 = [-0.3365, 0.9501, 0.8913, -0.7764, 0.0185, 0.4447, 0.7919, -0.9218, -0.9355, 0.0579]$$

The output of the system has been arbitrary chosen as being: $y = x^{10}$.

P-VALUE	PROPORTION	STATISTICAL TEST
0.911413	99/100	Frequency
0.759756	97/100	BlockFrequency
0.897763	100/100	CumulativeSums
0.122325	99/100	Runs
0.474986	99/100	LongestRun
0.911413	97/100	Rank
0.366918	99/100	FFT
0.419021	97/100	NonOverlappingTemplate
0.334538	99/100	OverlappingTemplate
0.935716	100/100	Universal
0.816537	98/100	ApproximateEntropy
0.128379	63/63	RandomExcursions
0.654467	61/63	RandomExcursionsVariant
0.554420	98/100	Serial
0.678686	99/100	LinearComplexity

Table 4: NIST test for the 4^{th} order system (2), "1 out of 10" under-sampling and 1-bit binarization

P-VALUE	PROPORTION	STATISTICAL TEST
0.213309	100/100	Frequency
0.108791	98/100	BlockFrequency
0.075719	100/100	CumulativeSums
0.719747	100/100	Runs
0.108791	100/100	LongestRun
0.816537	98/100	Rank
0.946308	98/100	FFT
0.115387	99/100	NonOverlappingTemplate
0.798139	98/100	OverlappingTemplate
0.058984	100/100	Universal
0.616305	98/100	ApproximateEntropy
0.054199	60/60	RandomExcursions
0.232760	59/60	RandomExcursionsVariant
0.437274	99/100	Serial
0.401199	100/100	LinearComplexity

Table 5: NIST test for the 10^{th} order Lozi function (2) and 1-bit binarization

The improvement of random properties of both strategies has been corroborated by the experimental results.

4 Conclusion

Classical and emergent applications (chaotic encryption, global warming, multi-agent competition) require efficient PRNG generating independent and multi-random sequences. A new alternate ring-coupled map confined to the torus has been proposed as a pseudo random number generator. Unlike the previous model, here the chaotic attractor is everywhere dense and there are no holes inside, in this way all output values are supposed to appear with the same probalility. Therefore, the new alternate Lozi function proposed in this paper has proved to be more efficient than the first one (without alternation of the coefficients). Moreover, the fourth order system has been analyzed and all the NIST tests for randomness have been successfull for the representative test sequences. Finally, a higher order system and an under-sampling of the output signal has been added and the results have shown to be very satisfactory.

By consequence, the proposed PRNG could be used succesfully for encryption and many other emerging applications wherever a multi-random number generator is required.

References

[1] A. Espinel, I. Taralova, R. Lozi, "Dynamical and Statistical Analysis of a New Lozi Function for Random Numbers Generation," *PHYSCON 2011*, León, Spain, 5 − 8 September, 2011.

[2] S. Hénaff, I. Taralova, R. Lozi, "Statistical and spectral analysis of a new weakly coupled maps system", *Indian Journal of Industrial and Applied Mathemaics*, vol 2. N2, pp. 1-18 (to appear).

[3] J. Jeanne, N.E. Lenoard and D. Paley, "Collective motion of ring-coupled planar particles", in *Proc. of the IEEE Conf. Decision Contr.*, pp.3929-3934, 2005.

[4] W. Kahan, "IEEE Standard 754 for Binary Floating Point Arithmetic, *Lecture Notes on the Status of IEEE 754*, Elect. Eng. & Computer Science University of California, Berkeley CA 94720-1776, May 1996.

[5] R. Lozi, "Giga-Periodic Orbits for Weakly Coupled Tent and Logistic Discretized Maps", *Modern Mathematical Models, Methods and Algorithms for Real World Systems*, A.H. Siddiqi, I.S. Duff and O. Christensen (Editors), Anamaya Publishers, New Delhi, India, 80-14, 2006. Proc. Conf. Intern. on Industrial and Appl. Math., New Delhi, India 4-6 Dec. 2004. Invited conference.

[6] R. Lozi, "Random properties of ring-coupled tent maps on the torus", submitted to *Discrete and continuous Dynamical Systems Series-B*.

[7] R. Lozi, "New enhanced chaotic number generators", *Indian Journal of Industrial and Applied Mathematics*, vol.1, pp. 1-23, 2008.

[8] R. Lozi and E. Cherrier, "Noise-resisting ciphering based on a chaotic multi-stream pseudo-random number generator", *6th International Conference on Internet Technology and Secured Transactions*, Abu Dhabi, UAE, pp. 91-96, December 2011.

[9] MATLAB R2009a (Online), *http://www.mathworks.com/*

[10] A. Srinivasan, M. Mascagni and D. Ceperley, "Testing parallel random number generators", *Parallel Computing*, vol.29, issue 1, pp. 69-94, 2003.

[11] A. Rukhin, et al, "A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications", *NIST (2001)*, http://csrc.nist.gov/rng/.

[12] I. Vattulainen et al. "A comparative study of some pseudorandom number generators", *Computer Physics Communications*, vol.86, issue 3, pp. 209-226, 1995.