THE PUBLISHING HOUSE
OF THE ROMANIAN ACADEMY

PROCEEDINGS OF THE ROMANIAN ACADEMY, Series A,
Volume 16, Special Issue 2015, pp. 357-366

A NEW CHAOTIC DYNAMICAL SYSTEM AND ITS USAGE IN A NOVEL PSEUDORANDOM NUMBER GENERATOR WITH A LINEAR FEEDBACK REGISTER STRUCTURE

Ana Cristina DASCALESCU, Radu BORIGA

Titu Maiorescu University, Faculty of Informatics, Department of Informatics, Romania
E-mail: cristina.dascalescu@prof.utm.ro

In this paper we propose a new chaotic discrete dynamical system and we prove, theoretically and numerically, its complex behavior, using Lyapunov exponent, bifurcation diagram and fractal dimensions of the attractor. Then, we use the proposed chaotic dynamical system in a new pseudorandom number generator having a structure similar to a linear feedback register. In the end, we present the results of its statistical and randomness analysis. The very good results obtained qualify the proposed pseudorandom number generator for use in cryptographic and simulation applications.

Key words: pseudorandom number generator, chaotic dynamical system, Lyapunov exponent.

1. INTRODUCTION

The relation between chaos and cryptography has become more and more attractive in the cryptography community, since the chaotic dynamical system possess some features, such as a high sensitivity to the initial condition, ergodicity, mixing property and structural complexity. Those properties can actually fulfill the based requirements postulated by Shannon regarding the security of a cryptosystem, i.e., confusion and diffusion [1]. Even if the dynamical systems are chaotic, their behavior is, still, deterministic. This was the main idea used by Oishi and Inoue [2] in 1982, when they developed a new pseudorandom number generator (PRNG) based on arbitrary Kolmogorov entropy. Since then, many researchers have proposed new chaos based pseudorandom number generators: Gonzalez and Pino [3] using the logistic map, Li in [4] based on the piecewise-linear map, Patidar in [5] involving the chaotic standard map and so on [6 – 12]. Some of the proposed pseudorandom number generators have shown a series of drawbacks, such as the predictability of generated values induced by the usage of a single chaotic orbit or a non-uniformity of the outputs caused by the improperly chose of the control parameters values [13 – 15].

Motivated by the extent of previous work, this paper aims to present a new chaotic discrete dynamical system which, furthermore, is included in a new PRNG, having a linear feedback register structure.

The paper is organized as follows: Section 2 presents the proposed dynamical system, including its chaotic behavior assessment; Section 3 presents the design of the new PRNG scheme, Section 4 presents the results of analysis performed using NIST suite, in order to test the randomness and the uniform distribution of values generated by the new PRNG. Finally, Section 5 summarizes the work carried out.

2. THE PROPOSED CHAOTIC DYNAMICAL SYSTEM

In order to obtain a large parameter's values space for which a dynamical system is in a chaotic regime, we proposed in [16] a new model for chaos generation, defined as:

$$x_{n+1}=h(f(x_n)), \tag{1}$$

Where *f* represents a periodic real map, selected to ensure a large phase space, while *h* represents a bounded map.

Therefore, the proposed discrete dynamical system, defined with respect to (1), is given by:

$$x_{n+1}=f(x_n),$$
$$f:[0,\pi]\to[0,\pi], \qquad f(x)=\arccos\left(\frac{\sin(rx)+r^2\cos(rx)}{1+r^2}\right) \tag{2}$$

where *r* is the control parameter.

Next, the dynamical behavior of the proposed chaotic system is investigated, by both theoretical analysis and numerical simulation [17, 18] (e.g., by means of Lyapunov exponent, attractor's geometric shape and fractal structure, bifurcation diagram, etc.).

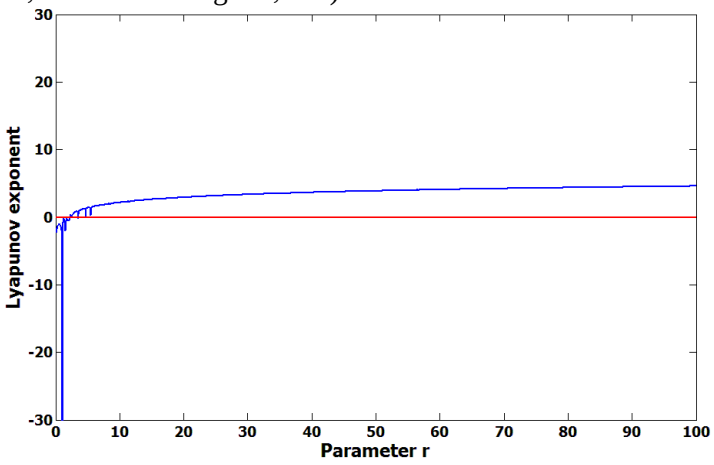

Fig. 1 – Lyapunov exponent of the proposed map.

A strong instrument used for the time behavior analysis is the *Lyapunov exponent*, which indicates the exponential divergence of two orbits starting from two close points in the phase space [17, 18]. If the map has a positive exponent, then the dynamical system is in a chaotic regime [17]. In practice, the Lyapunov exponents can be calculated numerically using the Wolf's algorithm [19]. In Fig. 1 are plotted the values of the Lyapunov exponent of an orbit for parameter $r\in[0,100]$.

It can be seen from the figure above that an orbit which starts from an initial point has a chaotic behavior for any value of the parameter $r\geq 5.5$.

THEOREM 1. *Let* $f:[0,\pi]\to[0,\pi]$ *be the map, defined by the relation* (2). *Then, for any control parameter* $r\geq 5.5$ *the map f is chaotic*.

Proof: For an orbit $\{x_1,\dots,x_k\}$ of the chaotic map *f*, the Lyapunov exponent λ_f is given by the relation [17]:

$$\lambda_f=\lim_{n\to\infty}\frac{1}{n}\sum_{i=1}^{n}\ln|f'(x_i)|=\lim_{n\to\infty}\frac{1}{n}\sum_{i=1}^{n}\ln\left|-\frac{r[\cos(rx_i)-r^2\sin(rx_i)]}{\sqrt{(r^2+1)^2-[\sin(rx_i)+r^2\cos(rx_i)]^2}}\right|=$$
$$=\ln r+\underbrace{\lim_{n\to\infty}\frac{1}{n}\sum_{i=1}^{n}\ln\left|\frac{\cos(rx_i)-r^2\sin(rx_i)}{\sqrt{(r^2+1)^2-[\sin(rx_i)+r^2\cos(rx_i)]^2}}\right|}_{L}, \tag{3}$$

In order to calculate the limit *L*, we applied a chi-square test in conjunction with a Monte Carlo analysis [20] over 1000 sets of points $\{x_1,x_2,\dots,x_{100000}\}$, and we proved that the values extracted from an orbit are uniformly distributed in the interval $[0,\pi]$. Thus, we obtain:

$$L = \lim_{n\to\infty}\frac{1}{n}\sum_{i=1}^{n}\ln\left|\frac{\cos(rx_i) - r^2\sin(rx_i)}{\sqrt{(r^2+1)^2 - [\sin(rx_i) + r^2\cos(rx_i)]^2}}\right| = \int_0^{\pi}\ln\left|\frac{\cos(rx) - r^2\sin(rx)}{\sqrt{(r^2+1)^2 - [\sin(rx) + r^2\cos(rx)]^2}}\right|dx \quad (4)$$

Using trapezoidal numerical integration (Fig. 2) we found the following approximation of the integral from the right term of the relation (4):

$$L = \int_0^{\pi}\ln\left|\frac{\cos(rx) - r^2\sin(rx)}{\sqrt{(r^2+1)^2 - [\sin(rx) + r^2\cos(rx)]^2}}\right|dx \in (-0.15, -0.02), \forall\, r \geq 5.5 \quad (5)$$

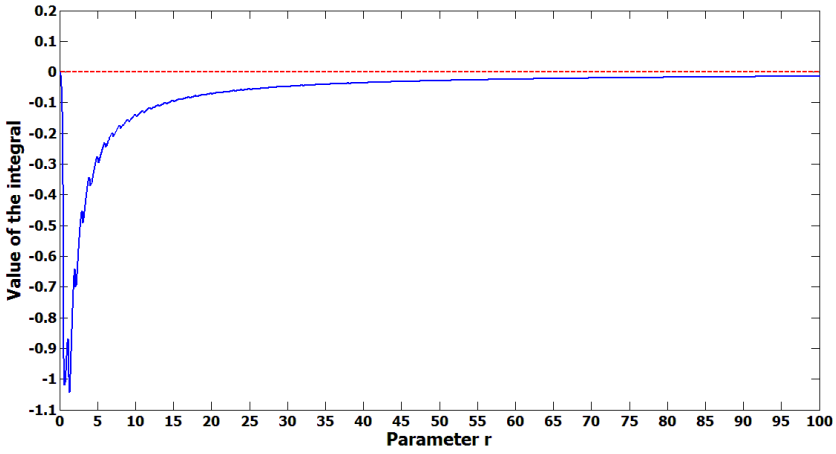

Fig. 2 – Numerical approximation of integral L.

Thus, from relation (5) we obtain:

$$\lambda_f = \ln r + L \geq \ln r - 0.15 > 0, \forall\, r \geq 5.5. \quad (6)$$

From the relation (6) we can conclude that the Lyapunov exponent of the proposed map is positive for any value of the control parameter $r \geq 5.5$, so the map is chaotic for any $r \geq 5.5$. ■

The time evolution of an orbit can be also represented using another instrument for chaos theory, the *bifurcation diagram*, which represents the set of all attractors (Fig. 3) in respect to the control parameter [17, 18].

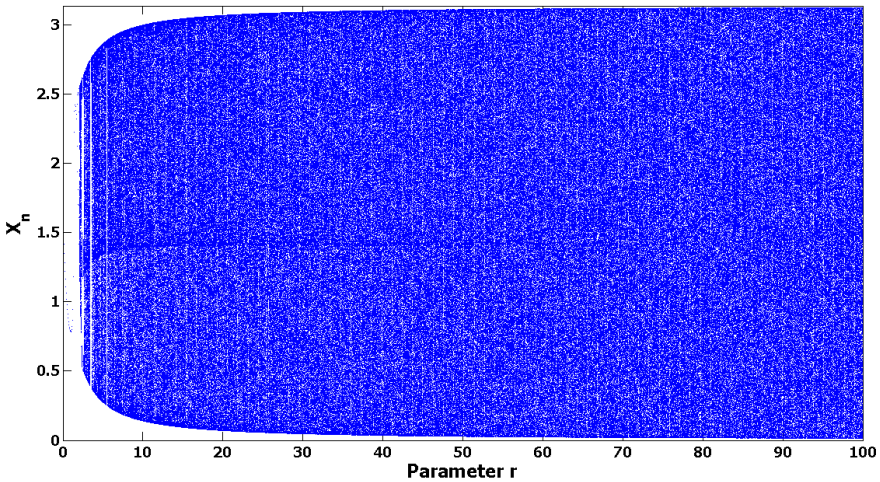

Fig. 3 – Bifurcation diagram of the proposed map.

It can be observed that for a value of the parameter $r \geq 2.1$, the f map has an instable behavior and for the parameter $r \geq 5.5$ the map enters in a complete chaotic regime.

The road to chaos of the f map with parameter $r \geq 5.5$ is not achieved through the doubling process of the period, specific to some chaotic maps [17], but is induced by the existence of a dense periodic orbits of any period in the phase space $[0, \pi]$.

Also, the analysis of the attractor's geometric shape of a dynamical system [17] can provide information about its behavior, for certain values of its control parameter. An attractor specific for a chaotic dynamical system has a complex fractal structure, while for a periodic dynamical system the attractor has a regular shape [17]. In Fig. 4 is represented the attractor of the f map for r=10.

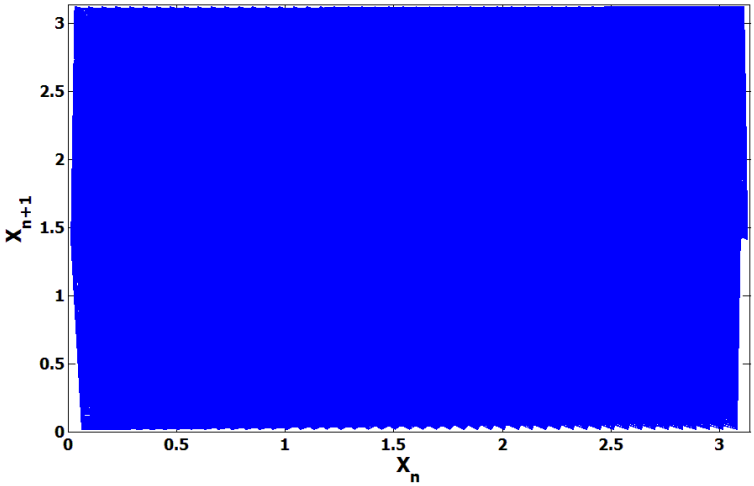

Fig. 4 – The attractor of the proposed map for r=10.

The fractal structure of an attractor is indicated by a fractional value of its fractal dimension, which is a measure of the complexity of a self-similar geometric shape. The fractal dimensions commonly used are box-counting dimension, Hausdorff dimension, information dimension and correlation dimension [21-23]. Using the plots from Fig. 5 and Fig. 6, we established that the attractor of the f map has a box-counting dimension D_B=1.9151 and a correlation dimension D_C=1.9172.

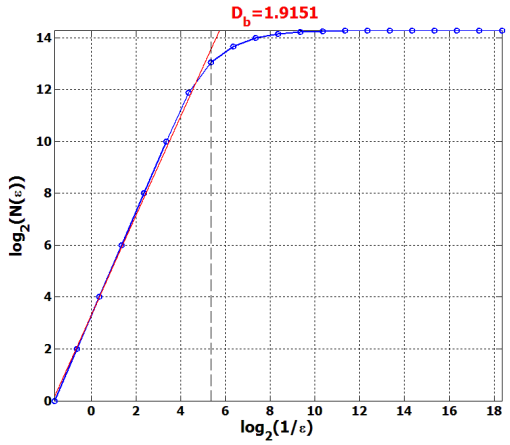

Fig. 5 – Box-counting dimension of the attractor $D_B \approx 1.9151$.

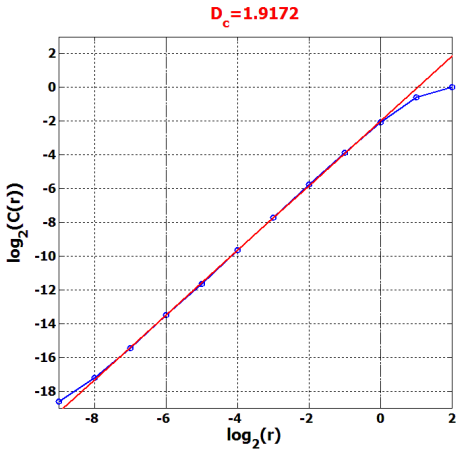

Fig. 6 – Correlation dimension of the attractor $D_C \approx 1.9172$.

The fractional values of these fractal dimensions lead us to the conclusion that the proposed map has a strange attractor, which indicates an underlying chaotic behavior.

Summing up, the obtained results prove that the proposed map has a chaotic behavior for a very large parameter values interval (i.e., for any value ≥5.5), in comparison to the well-known chaotic maps [17, 18]

such as logistic map (i.e., for $r \in [3.9,4]$) tent map (i.e., for $r \in [0.9,1)$), etc. So, the proposed chaotic map is suitable for chaos-based cryptographic applications.

3. THE PROPOSED PRNG

In the case of chaos-based PRNGs, the security issues are typically caused either by predictability of the values extracted from a single orbit of the involved chaotic map, or by the choice of its control parameters from a narrow values interval [13 – 15], which, because of discretization effects, can lead to a degradation of the chaotic behavior to a stable one (e.g., the logistic map has some "islands of stability" around the values 3.63, 3.74 and 3.82 of the control parameter, even it has a chaotic behavior starting from the value 3.57 of the control parameter [17, 18]).

The proposed PRNG has a linear feedback register structure, based on 32 chaotic maps of type (2), having different values of control parameters. The current value, initialized with the seed, is passed circularly through each of the 32 chaotic maps. After each group of 4 chaotic maps, the current value is discretized to an unsigned integer, which is bitwise rotated by a random number of positions and, afterwards, it's outputted. Moreover, the control parameter of the next chaotic map will be dynamically altered by adding the sum of some of the previously chaotic maps outputs, selected using a binary mask. Thus, the unpredictability and the sensitivity to the initial conditions of the proposed PRNG is very high.

In this way, the proposed PRNG highly ameliorates both shortcomings above mentioned. Each output is obtained from multiple compounded chaotic orbits and, moreover, is altered by a bitwise rotation. The usage of chaotic maps of type (2) guarantees a full chaotic regime, without "islands of stability", for any value of the control parameter greater than 5.5, allowing a safe selection of control parameters from a very large interval of values.

Next, we will denote by $ChaoticMap(r,x)$ a subprogram which implements a chaotic map of type (2), by $GetBit(x,i)$ a subprogram which returns the bit $i \in \{0,1,\ldots,31\}$ of a 4-bytes unsigned integer x, by $RotR(x,n)$ a subprogram which returns the value of an unsigned integer x after a circular shift of its bits with n positions, and by $Floor(x)$ the largest integer less than or equal to the real number x.

Thus, the proposed algorithm for generating pseudorandom numbers is as it follows:

Algorithm 1. The proposed pseudorandom number generator

INPUT: unsigned integers n (number of random unsigned integers to be generated) and m (the binary mask), real number x_0 (initial value, chosen from the interval $[0,\pi]$), array $p[0..31]$ of real numbers (control parameters of the chaotic maps, chosen so to ensure a chaotic behavior, i.e. greater than 5.5)

$x[0] \leftarrow x_0$
$aux \leftarrow m \bmod 32$
$s \leftarrow 0$
$k \leftarrow 0$
while $k < n$ **do**
  $i \leftarrow 1$
  while $(i < 32)$ **and** $(k < n)$ **do**
    $x[i] \leftarrow ChaoticMap(p[i], x[i-1])$
    $s \leftarrow s + GetBit(m,i) * x[i]$
    if $i \bmod 4 = 3$ **then**
      $v[k] \leftarrow RotR(Floor(10^{15} * x[i]) \bmod 2^{32}, aux)$
      $aux \leftarrow v[k] \bmod 32$
      $k \leftarrow k + 1$
      $p[(i+1) \bmod 32] \leftarrow p[(i+1) \bmod 32] + s$
    end if
    $i \leftarrow i + 1$
  end while
  $x[0] \leftarrow x[31]$
end while

OUTPUT: array $v[0..n-1]$ of random unsigned integers

A logic diagram of the proposed algorithm is presented in Fig. 7.

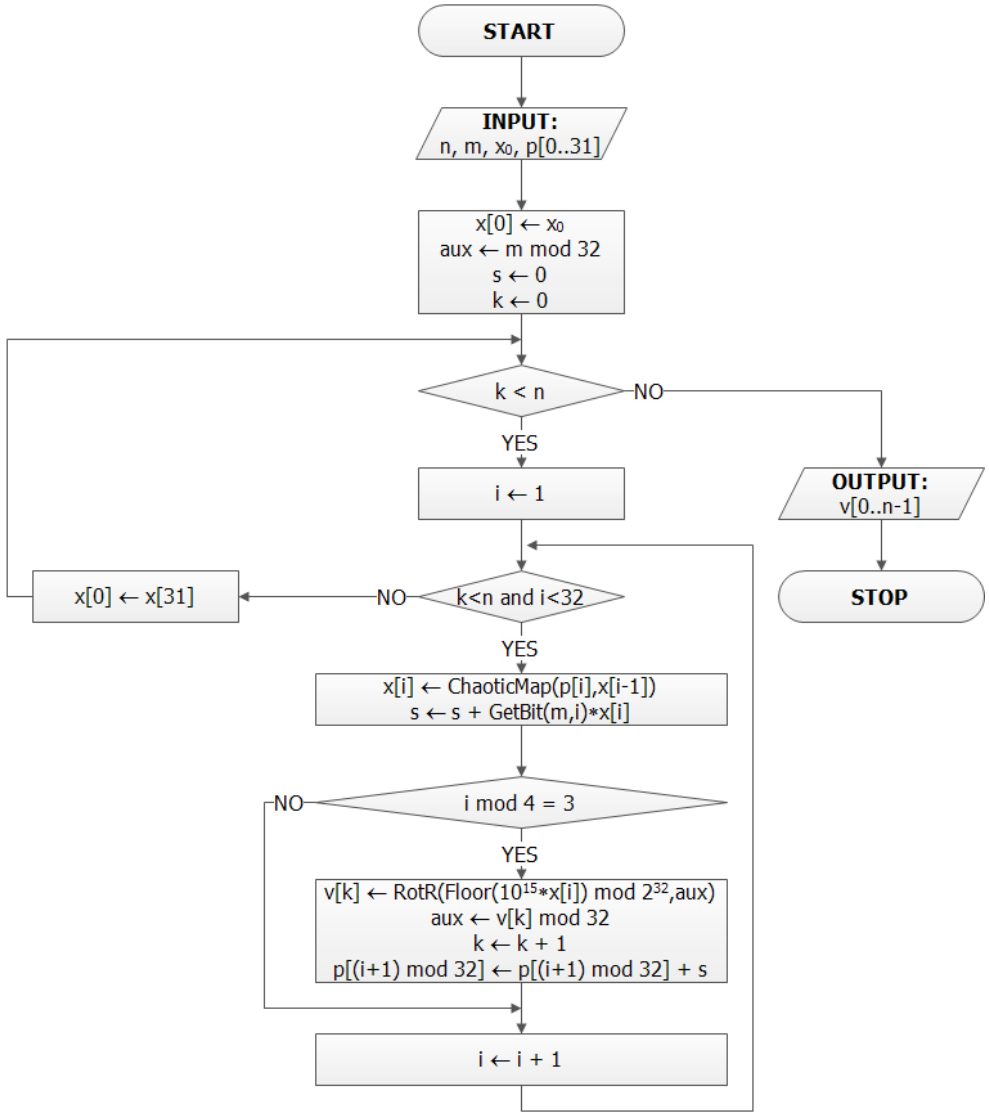

Fig. 7 – The logic diagram of the proposed algorithm.

Obviously, the asymptotic computational complexity of the proposed algorithm it's a linear one in terms of number n of random unsigned integers to be generated, i.e. $\Theta(n)$, so it can be considered as a very fast one. Experimentally, the proposed PRNG have proved an average speed around 10 MB/s, confirming its fastness.

Moreover, the proposed PRNG is scalable, allowing the use of an arbitrary number of chaotic maps of type (2) (with the only restriction that it must be multiple of 4) and is suitable for implementation using parallel programming.

4. PERFORMANCES ANALYSIS OF THE PROPOSED PRNG

4.1. Seed space

One of the most common applications of PRNGs is the use in cryptographic applications to generate encryption keys. In this case, the initial conditions of the PRNG will be embedded in the secret key of the

cryptographic application, decisively influencing its security. For this reason, a PRNG must have a large seed space, in order to prevent an attack by brute-force.

The seed of the proposed PRNG consists from 33 real numbers (an initial value and 32 control parameters of the involved chaotic maps) and an unsigned integer (the binary mask). The implementation of the PRNG must use a real data type having a high precision, in order to prevent the negative effects of the discretization. If the implementation of the cryptosystem uses a programming language that complies with *IEEE Standard 754-2008* [24], then we recommend the double data type, which stores real numbers on 8 bytes, with an accurate of 15 decimal places. In this case, the size of the seed space will be equal to $2^{2144} \approx 2.56 \times 10^{645}$, a large enough value to prevent guessing of the initial conditions by a brute-force attack in a useful time.

4.2. Statistical testing

Before testing the randomness of the values generated by the proposed PRNG, we performed a standard statistical analysis, based on well-known indicators, such as: mean value, variance, standard deviation, skewness, kurtosis and entropy [20]. In this scope, we generated m=1000 different binary sequences, obtained from 1000 randomly chosen seeds, each sequence having length n=1000000 bytes and we performed the statistical analysis at byte level (i.e., considering every byte as an unsigned integer between 0 and 255). The average values obtained are summarized in Table 1.

Table 1

Statistics of the proposed PRNG

Mean	Standard deviation	Variance	Skewness	Excess kurtosis	Entropy
127.4688	73.9037	5461.8	-0.0000961	-1.2003	7.9998

From Table 1 it can be observed that the mean has a value very close to the ideal of 128, while the high values of standard deviation and variance shows a spreading of the bytes over the whole range of values $\{0, 1, \ldots, 255\}$. Moreover, the value very close to 0 of the skewness indicates a symmetric distribution of the values around the mean [20 – 25], while a negative excess kurtosis denotes a distribution with flatter peak around the mean [20 – 26]. Summing up, the bytes generated by our PRNG have an uniform distribution, along with a very high degree of uncertainty, proved by the value of entropy very close to the ideal value of 8 [1].

4.3. Randomness testing

In order to analyze the randomness of the values generated by the proposed PRNG, we use *The NIST Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications* [27], a statistical package of 15 tests developed to test the randomness of binary sequences produced by a PRNG, all being focused on different types of non-randomness that could exist in a binary sequence. Each test produces a *P-value*, which is a real number between 0 and 1. If the *P-value* is greater than a significance level α, by default equal to 0.01, then the binary sequence passes the test, so the sequence may be considered to be random with a confidence of 99%. Moreover, if the tested binary sequences are random, then the *P-values* must be uniformly distributes in the interval [0,1). The *P-value*$_T$ corresponding to the uniformity of the *P-values* must to be greater than 0.0001 so as the *P-values* to be considered uniformly distributed [27].

In our statistical experimentations we used m=2000 different binary sequences, each sequence of length n=1000000 bits. The acceptance region of the passing ratio is $\left[p - 3\sqrt{\frac{p(1-p)}{m}}, p + 3\sqrt{\frac{p(1-p)}{m}}\right]$, where m is the number of tested binary sequences and p=1-α is the probability of passing each test [27]. For m=2000 and the probability p=0.99 (corresponding to the default significance level α=0.01) the confidence interval is [0.983, 0.996].

In Table 2 we summarized the results of the testing process performed by the NIST suite. From the second column of the table it can be observed that the passing ratio of each test lies inside the confidence interval [0.983, 0.996], while from the third column it can be observed the uniform distribution of the *P-values* for each statistical test, so we can conclude that all the binary sequences generated using the proposed PRNG are random with respect to all NIST tests.

Table 2

The results of the NIST tests

Test name	Passing ratio of the test	P-value for uniformity	Result
Frequency	0.989500	0.643366	SUCCESS
Block Frequency	0.992000	0.362765	SUCCESS
Cumulative Sums	0.990000	0.324436	SUCCESS
Runs	0.991500	0.348869	SUCCESS
Longest Run	0.990500	0.428095	SUCCESS
Rank	0.988000	0.224821	SUCCESS
FFT	0.986000	0.557481	SUCCESS
Non-Overlapping Template	0.985000	0.663130	SUCCESS
Overlapping Template	0.993500	0.833436	SUCCESS
Universal	0.986500	0.013953	SUCCESS
Approximate Entropy	0.989000	0.863690	SUCCESS
Random Excursions	0.983512	0.644003	SUCCESS
Random Excursions Variant	0.985161	0.582224	SUCCESS
Serial	0.988500	0.234981	SUCCESS
Linear Complexity	0.990000	0.899871	SUCCESS

In conclusion, all the results obtained shows that the proposed PRNG is fast and has a very large seed space, and, the most important, generates random values with an uniform distribution, which qualifies it for use in cryptographic and simulation applications.

4.4. Strict avalanche criterion randomness test

Firstly, the Strict Avalanche Criterion (SAC) was proposed in [28] for measuring the amount of non-linearity in substitution boxes used in block ciphers (e.g. AES and DES). In this sense, it estimates the amount of change in the output sequence when the key is changed by one bit. Mathematically, a mapping $\mathbf{F}$ having a $\mathbf{n}$-bit output from an input satisfies SAC if:

$$\forall x | \forall y \text{ such that } H_{wt}(y) = 1, \qquad H_{dist}(F(x), F(x \oplus y)) \approx \frac{n}{2} \tag{7},$$

where H_{wt} denotes the Hamming weight and H_{dist} denotes the Hamming distance [29].

Castro et al. proposed in [30] a new definition of SAC for randomness testing of a PRNG, interpreting the Hamming distances between *F(x)* and $F(x \oplus y)$ as a random variable and stated that it should follow the Binomial distribution $\mathrm{B}(1/2, n)$:

$$\forall x, y |\ H_{dist}(x, y) = 1, \qquad H_{dist}\big(F(x), F(y)\big) \approx \mathrm{B}\left(\frac{1}{2}, n\right) \tag{8}$$

The test is applied on the PRNG output, interpreted as sequence of n-bit blocks ($n \in \{8, 16, 32, 64, 128\}$) and the distribution of Hamming distances between pairs of adjacent blocks is observed. The closeness of this distribution with *B(1/2, n)* is measured using the chi-square goodness-of-fit test. If the observed distribution is close to the expected one, the sequence is considered to pass the test.

In our SAC testing process we used the same *m*=2000 different binary sequences, each sequence of length 1000000 bits, used in NIST randomness tests described above. In Table 3 we summarized the average results of the SAC tests, considering a 0.05 significance level.

Table 3

The results of the SAC tests

Block length (n)	**Chi-square goodness-of-fit test**		**Result**
	Obtained value	**Expected value**	
8	9.2714	15.5073	SUCCESS
16	12.4437	26.2962	SUCCESS
32	28.7903	46.1943	SUCCESS
64	49.7318	83.6753	SUCCESS
128	53.7717	155.4047	SUCCESS

In conclusion, the obtained results shows that the proposed PRNG passes the SAC randomness test for all block lengths of $n \in \{8, 16, 32, 64, 128\}$, so it possesses a high degree of unpredictability of the generated values.

4.5. Speed test

An important factor to be taken into account in the performance evaluation of a PRNG is the speed. In this sense, we run the proposed algorithm, implemented in C language, under Windows 8.1, using a PC with Intel(R) Core(TM) i3 @2.53GHz CPU and 4GB RAM. In Table 4 we compare the mean speed of the proposed PRNG with the speeds of other chaos-based PRNGs.

Table 4

Speed performances

PRNG	**Speed (MB/s)**
Our PRNG	29.12
Ref. [31]	3.88
Ref. [32]	3.33

Analyzing the speeds from Table 4, we can say that the proposed PRNG is a fast one, with a mean speed of 30 MB/s, which is better than other chaos-based proposed PRNGs.

5. CONCLUSIONS

In this paper, firstly we proposed a new discrete chaotic dynamical system and, using the Lyapunov exponent and other chaos theory tools, we proved that it has a chaotic behavior for a very large control parameter values interval. Secondly, this important feature of the proposed chaotic dynamical system is exploited in a new PRNG schema having a linear feedback register structure, allowing a dynamic alteration of the control parameters values of some involved chaotic maps. Finally, we presented the results of the statistical and randomness testing performed on the values outputted by the proposed PRNG. The very good results obtained, along with its simplicity and high speed, qualify the proposed PRNG schema for use in cryptographic and simulation applications.

REFERENCES

1. C.E. SHANNON, *A mathematical theory of communication*, Bell Systems Technical Journal, **27**, *3*, pp. 379-423, 1948.
2. S. OISHI, H. INOUE, *Pseudo-random number generators and chaos*, Transactions of the Institute of Electronics and Communication Engineers of Japan, **65**, pp. 534-541, 1982.
3. J.A. GONZALEZ, R. PINO, *Random number generator based on unpredictable chaotic functions*, Computer Physics Communications, **120**, pp. 109-114, 1999.
4. S. LI, X. MOU, Y. CAI, *Pseudo-random bit generator based on couple chaotic systems and its application in stream-ciphers cryptography*, Lecture Notes in Computer Science, **2247**, pp. 316-329, 2001.
5. V. PATIDAR, K.K. SUD, *A novel pseudo random bit generator based on chaotic standard map and its testing*. Electronic Journal of Theoretical Physics, **20**, pp. 327-344, 2009.
6. N.K. PAREEK, V. PATIDAR, K.K. SUD, *A random bit generator using chaotic maps*, International Journal of Network Security, **10**, *1*, pp. 32-38, 2010.
7. A. LUCA, A. ILYAS, A. VLAD, *Generating random binary sequences using tent map*, Proceedings of the 10th International Symposium on Signals, Circuits and Systems (ISSCS '11), Iași, Romania, pp. 1–4, 2011.
8. X.Y. WANG, Y.X. XIE, *A design of pseudo-random bit generator based on single chaotic system*, International Journal of Modern Physics C, **23**, *3*, 2012.
9. X. ZHAO, F. JIANG, Z. ZHANG, J. HU, *A new series of three dimensional chaotic systems with cross-product nonlinearities and their switching*, Journal of Applied Mathematics, **2013**, Article ID 590421, 2013.
10. A.V. DIACONU, K. LOUKHAOUKHA, *An Improved Secure Image Encryption Algorithm Based on Rubik's Cube Principle and Digital Chaotic Cipher*, Mathematical Problems in Engineering, **2013**, Article ID 848392, 2013.
11. A. AKHSHANI, A. AKHAVAN, A. MOBARAKI, S.C. LIM, Z. HASSAN, *Pseudo random number generator based on quantum chaotic map*, Communications in Nonlinear Science and Numerical Simulation, **19**, *1*, pp. 101-111, 2014.
12. M. FRANCOIS, T. GROSGES, D. BARCHIESI, R. ERRA, *A new pseudo-random number generator based on two chaotic maps*, Informatica, **24**, *2*, pp. 181-197, 2013.
13. D. ARROYO, G. ALVAREZ, S. LI, C. LI, J. NUNEZ, *Cryptanalysis of a discrete-time synchronous chaotic encryption system*, Physics Letters A, **372**, *7*, pp. 1034-1039, 2008.
14. S. LI, X. MOU, B. L. YANG, Z. JI, J. ZHANG, *Problems with a probabilistic encryption scheme based on chaotic systems*, International Journal of Bifurcation and Chaos, **13**, *10*, pp. 3063-3077, 2003.
15. G. ALVAREZ, F. MONTOYA, M. ROMERA, G. PASTOR, *Cryptanalysis of an ergodic chaotic cipher*, Physics Letters A, **311**, *2-3*, pp. 172-179, 2003.
16. A.C. DASCAĂLESCU, R. BORIGA, A.V. DIACONU, *Study of a New Chaotic Dynamical System and Its Usage in a Novel Pseudorandom Bit Generator*", Mathematical Problems in Engineering, **2013**, Article ID 769108, 2013.
17. K.T. ALLIGOOD, T.D. SAUER, AND J.A. YORKE, *Chaos: An introduction to dynamical systems*, Springer-Verlag, 1996.
18. A. SERBAĂNESCU, C. I. RANCU, *Systemes et Signaux Face au Chaos: Applications aux Communications*, Military Technical Academy Publishing House, Bucharest, Romania, 2008.
19. A. WOLF, J.B. SWIFT, H.L. SWINNEY, J.A. VASTANO, *Determining Lyapunov exponents from a time series*, Physica D, **16**, pp. 285-317, 1985.
20. R.M. GRAY, *Probability, random processes, and ergodic properties*, Springer-Verlag, 2010.
21. J.D. FARMER, E. OTT, J.A. YORKE, *The dimension of chaotic attractors*, Physica D, **7**, *1-3*, pp. 153-180, 1983.
22. P. GRASSBERGER, I. PROCACCIA, *Measuring the strangeness of strange attractors*, Physica D, **9**, *1-2*, pp. 189-208, 1983.
23. J. THEILER, *Efficient algorithm for estimating the correlation dimension from a set of discrete points*, Physical Rev. A, **36**, *9*, pp. 4456-4462, 1987.
24. *IEEE Standard for Floating-Point Arithmetic*, IEEE Standard 754-2008, pp. 1-70, 2008.
25. D.P. DOANE, L.E. SEWARD, *Measuring skewness: a forgotten statistics?*, Journal of Statistics Education, **19**, *2*, pp. 45-63, 2011.
26. L.T. DECARLO, *On the meaning and use of kurtosis*, Psychological Methods, **2**, *3*, pp. 292-307, 1997.
27. A. RUKHIN, J. SOTO, J. NECHVATAL, M. SMID, E. BARKER, S. LEIGH, M. LEVENSON, M. VANGEL, D. BANKS, A. HECKERT, J. DRAY, S. VO, *A statistical test suite for the validation of random number generators and pseudo random number generators for cryptographic applications*, NIST Special Publication 800–22, 2010.
28. R. FORRE, *The strict avalanche criterion: spectral properties of booleans functions and an extended definition*, in: *Advances in cryptology*, Lecture Notes in Computer Science, **403**, pp. 450–468, 1990.
29. J.C.H. CASTRO, J.M. SIERRA, A. SEZNEC, A. IZQUIERDO, A. RIBAGORDA, *The strict avalanche criterion randomness test*, Mathematics and Computers in Simulation, **68**, pp. 1-7, 2005.
30. P.R. MISHRA, I. GUPTA, N.R. PILLAI, *Generalized Avalanche Test for Stream Cipher Analysis*, in: *Security Aspects in Information Technology*, Lecture Notes in Computer Science, **7011**, pp. 168-180, 2011.
31. L. YANG, T. XIAO-JUN, *A new pseudorandom number generator based on complex number chaotic equation*, Chinese Physics B, **21**, *9*, pp. 1-7, 2012.
32. S. AHADPOUR, Y. SADRA, Z. ARASTEH-FARD, *A Novel Chaotic Image Encryption using Generalized Threshold Function*, International Journal of Computer Applications, **42**, *18*, pp. 25-31, 2012.