A NEW CHAOTIC MAP SUITABLE FOR USING IN CRYPTOGRAPHIC APPLICATIONS

Cristina FILIS[1], Marius Iulian MIHĂILESCU[2]
[1,2]Titu Maiorescu University, Faculty of Informatics, Romania
[1]cristina.filis@prof.utm.ro, [2]marius.mihailescu@prof.utm.ro

Keywords: chaotic map, chaos based cryptography, Lyapunov exponent, bifurcation diagram, strange attractor, fractal dimension

Abstract: *Chaotic cryptography has been widely studied in the last 20 years. A common feature in most of the proposed chaotic cryptosystems is the use of a single dynamical map in the encoding–decoding process, fact which leads to a low level security of its. In this paper we propose a new dynamical system based on transcendental equations suitable for secure encryption scheme. Its good cryptographic properties are proved using some specific tools from chaos theory, such as Lyapunov exponent, bifurcation diagram and attractor. In addition, we present a randomness test using the standard statistical test, the NIST battery.*

1. INTRODUCTION

Although chaos implies unpredictable time behaviour of a system, its dynamics, whose evolution seems to be random, can be expressed by a deterministic rule. This is one of the main properties of chaotic dynamical systems which have encouraged the idea to design new pseudorandom number generators and also to develop some robust encryption schemes based on chaos. In addition, some specific properties of chaotic systems, such as ergodicity, sensitivity to initial conditions and mixing properties can be connected with the notions of confusion and diffusion, introduced by Shannon [1]. Due this close relationship, in recent years have been proposed a number of cryptographic chaos-based schemes, which lead to a new research and development direction, generic namely chaotic cryptography [2].

Discrete dynamical systems are usually studied by means of their evolution, over time domain, which is given by the sequence of points $\{x_0, x_1, \dots, x_n\}$, called orbit, where $x_0, \dots, x_n \in U$ and x_k is defined by $x_{k+1} = f(x_k)$, for any $k = \overline{0, n-1}$. The chaotic systems used as base of cryptosystems are defined in a parametric way, such that their dynamics depends by one or several control parameters. Moreover, those chaotic systems are dynamical systems which show a chaotic behavior only for certain values of the associated control parameters. Therefore, the design of a cryptosystem based on any of those dynamical systems must be done by guaranteeing the use of a set of values for the control parameters which leads to chaos [3]. Also, in some chaos based encryption schemes, the confusion and/or diffusion properties depend on the probability distribution function of the orbits derived from the selected chaotic system. Therefore, to improve the security level of the chaotic dynamical systems, we must to ensure the ergodicity property, too.

In the last decade many chaos encryption scheme has been put forward [4 - 11]. The most used map in those encryption schemes are the logistic map, tent map, PWCL map and Hénon map [7], [10], [12 - 16]. Yet, some security issues such as small key space, non-uniformity distribution and existence of some correlations between the plaintext and the encrypted one [12], [17-20] are still present. Due to this fact, most of the proposed cryptosystems were shown later to be unsecure against one or other type of attack, while the safer ones were typically too slow to compete with classic ciphers. This shortcoming,

of chaotic cryptography, it's mandatory to be removed, as to be considered a viable alternative to the classic cryptography.

Motivated by the extent of previous work, present article aims to present a new chaotic discrete dynamical system suitable for secure encryption scheme. Its good cryptographic properties are proved using some specific tools from chaos theory, such as bifurcation diagram, Lyapunov exponent and attractors. Moreover, the randomness of the values extracted from its orbits is tested with a standard statistical battery, i.e., NIST [21].

The very good obtained results prove that the proposed discrete chaotic dynamical system can be used in cryptographic applications, as stand-alone pseudorandom number generator or for generating key-streams.

2. DESCRIPTION OF THE PROPOSED DYNAMICAL SYSTEM

Newly dynamical system introduced in paper uses (1) as model for chaos generation [11]. Here, whilst f represents a periodic real map (selected so as to ensure a large phase space), h represents a bounded real map (which, by an appropriate selection, restricts the phase space to a closed interval in which the dynamical system has good chaotic properties).

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

Therefore, the newly proposed one-dimensional discrete dynamical system, which is defined with respect to relation (1), is given by:

$$\begin{aligned} x_{n+1} &= f_P(x_n) \\ f_P&:\left[-\frac{\pi}{2},\frac{\pi}{2}\right] \to \left[-\frac{\pi}{2},\frac{\pi}{2}\right], \\ f_P(x) &= \operatorname{arctg}(\sin(2^r x) + x) \end{aligned} \tag{2}$$

Here, r represents the control parameter of resulted chaotic map, while arctg (i.e., arctangent function), resp., sin (i.e., sin function) where chosen with respect to the above affirmations (i.e., the first one restricts the phase space to a close interval in which the dynamical system has a good chaotic properties, while the second one ensures a large phase space) [11].

In the following, dynamical behaviour of newly proposed chaotic system is investigated, by numerical simulation using specific tools from chaos theory such as Lyapunov exponent, bifurcation diagram, attractor's geometric shape and fractal structure.

Behaviour, over time domain, of proposed discrete dynamical systems depends both on the control parameter r and the initial condition x_0. First of all, we propose stability analysis of fixed points, in order to assess system's sensitivity level to initial conditions [22].

The calculation the fixed points of f_G map involves the solving the nonlinear equation:

$$\operatorname{arctg}(\sin(2^r x) + x) = x \tag{3}$$

Since the equation (3) is transcendental its solutions cannot be determinate using analytical methods. Thus, the stability of fixed points can be analysed only with numerical methods.

A powerful numerical instrument is the bifurcation diagram which is a representation of attractors' sets of a dynamical system in respect to the control parameter. In the phase space, a fixed point which corresponds to a steady state can abruptly change its stability, while the values of control parameter changes. These qualitative changes are called bifurcations and the parameter values for which each of them occurs are called bifurcation values. In Fig. 1 we plotted the bifurcation diagram for f_G map with $r > 0$.

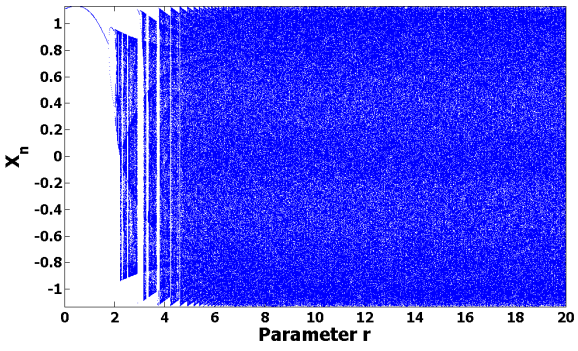

Fig. 1 *Bifurcation diagram of* f_P *map for* $r \in [0,20]$

From the bifurcation diagram (Fig. 1) it can be observed that for values of the control parameter $r \in [0,2)$ the f_P map has a periodic

behaviour. When the control parameter r reaches the value 2, the first doubling-period bifurcation point appears and, after that, for $r \in [2,6]$ the f_P map is in an intermittent chaotic regime. For values of the control parameter $r > 6$ the f_P map has a chaotic behaviour without periodic windows and it is also ergodic.

Another tool used to assess f_P map sensitivity to initial conditions is the Lyapunov exponent [22]. Lyapunov exponent, numerically computed, using Wolf's algorithm [23], with respect to the parameter r within $[0,20]$ interval, is showed in Fig. 2.

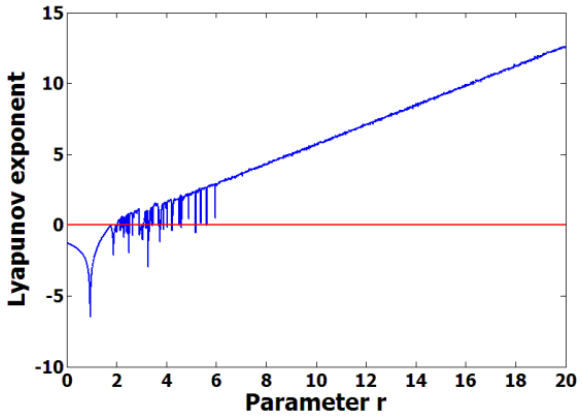

Fig. 2 Lyapunov exponent of f_P map for $r \in [0,20]$

Taking into consideration the fact that an orbit $\{x_1, x_2, \dots, x_n\}$ is chaotic if its exponent is positive, it can be seen that for any parameter $r > 6$ the f_P map is completely in a chaotic regime.

Analysis of the shape of a dynamical system's attractor can provide meaningful information about system behaviour in time, for certain values of its parameters. The attractor of a dynamical system with a periodic behaviour has a regular shape, while the one corresponding to a chaotic dynamical system has a complex structure, of fractal type, called strange attractor [22], [24].

In Fig. 3 is plotted the attractor of f_P map for $r = 10$. It can be observed that it has a complex shape, of fractal type.

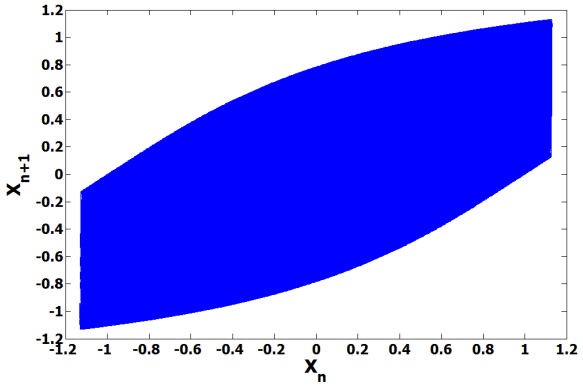

Fig. 3 Attractor of f_P map for $r = 10$

Fractal structure of an attractor is indicated by a non-integer value of its fractal dimension, which allows to measure the degree of complexity of a geometric shape by evaluating how fast its measurements increase or decrease as the scale becomes larger or smaller. There are several types of fractal dimensions, which can be theoretically and empirically estimated, such as Minkowski-Bouligand dimension, box-counting dimension, information dimension, correlation dimension and Hausdorff dimension [24 - 27]. Using the plot from Fig. 4, we established that the attractor of the f_P map has a box-counting dimension $D_b = 2.4534$ and using Fig. 5 we've calculated correlation dimension $D_c = 1.7214$. The fractional values obtained for both fractal dimensions allow us to conclude that the f_P map has a strange attractor which, at its turn, indicates a chaotic behavior.

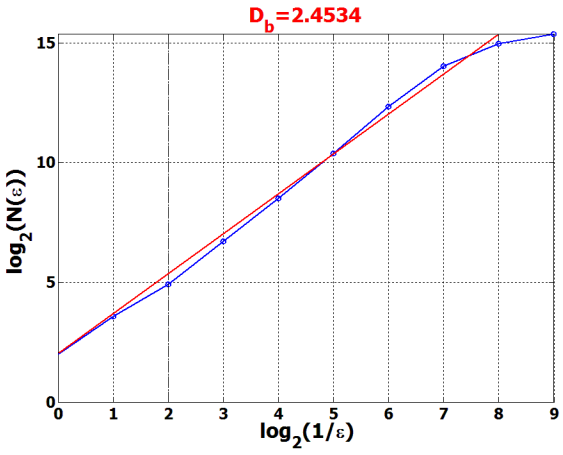

Fig. 4 Box-counting dimension of the attractor of the f_P map

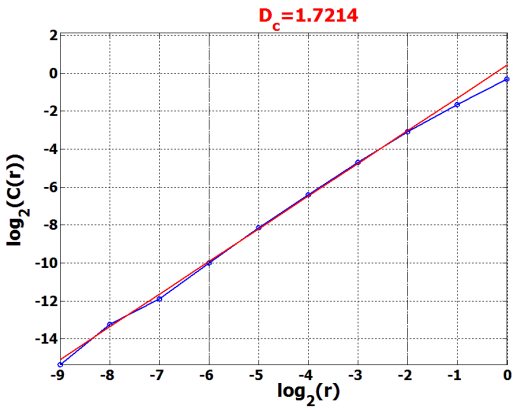

Fig. 5 Correlation dimension of the attractor of the f_P map

Concluding, the proposed dynamical system is chaotic for any value of the control parameter $r > 6$, so the induced secret keys' space is much larger than the one corresponding to others well-known chaotic maps (e.g. the logistic map has a chaotic regime without periodicity windows only for values of the control parameter between 3.9 and 4).

3. ANALYSIS OF THE RANDOMNESS

In order to test the security level of the system against some statistics cryptanalytic attacks, the evaluation of the properties of a dynamical system must include a statistical analysis of the randomness of the generated values. In this sense, the most used suite of statistical tests for randomness is NIST [21].

Next, we present the results obtained in the testing process of randomness of the binary sequences generated by the proposed map, using the NIST standard battery. For the numerical tests, we have generated $m = 2000$ different binary sequences from 500 randomly chosen seeds. Each sequence has length $n = 1000000$ bits and for all of them we computed the corresponding *p-value* for all the 15 tests of the NIST suite.

The significance level of each test in NIST is set to 1%, which means that 99% of test samples pass the tests if the random numbers are truly random. The acceptance region of the passing ratio is given by (4), where m represents the number of samples tested and $p = 1 - \alpha$ is the probability of passing each test [21].

$$\left[p - 3\sqrt{\frac{p(1-p)}{m}}, p + 3\sqrt{\frac{p(1-p)}{m}}\right] \qquad (4)$$

For $m = 2000$ and probability $p = 0.99$ (corresponding to significance level $\alpha = 0.01$) we obtained confidence interval [0.983,0.996].

In Table 1 we have summarized the results obtained after applying non-parameterized and parameterized tests of NIST suite on the binary sequences produced by proposed pseudorandom bit generator. In the column 2 it can be observed that the computed proportion for each test lies inside the confidence interval [0.983,0.996]. Hence, the tested binary sequences generated by the proposed map are random with respect to all tests of NIST suite. If the tested sequences are truly random, then the $p - values$ is expected to appear uniform in [0,1). NIST recommends to apply a χ^2- test in which the interval [0,1) is divided into 10 subintervals.

Defining F_i as number of occurrences of $p - value$ in i-th interval, then the value of the χ^2- test is given by (5).

$$\chi^2 = \sum_{i=1}^{10} \left(F_i - \frac{m}{10}\right)^2 / (m/10) \qquad (5)$$

NIST recommends to set its significance level to 0.01%, so as the acceptance region of statistics is $\chi^2 \leq 33.72$.

$p - value$ corresponding to uniformity of the $p - values$ is calculated with (6) and it must to be greater than 0.0001, as to ensure that the $p - values$ are (at least, could be considered) uniformly distributed.

$$igamc\left(\frac{9}{2}, \frac{\chi^2}{2}\right) \qquad (5)$$

Results from column 3, of Table 1, show that the $p - values$, for each statistical test, are uniformly distributed in the interval [0, 1].

Table 1 Results of the NIST randomness test

Test Name	Passing Ratio of the Test	Uniformity p-value	Result
Frequency	0.998	0.762303	SUCCESS
Block Frequency	0.992	0.345891	SUCCESS
Cumulative Sums	0.993	0.109078	SUCCESS
Runs	0.991	0.363005	SUCCESS
Longest Run	0.987	0.192443	SUCCESS
Rank	0.992	0.940867	SUCCESS
FFT	0.992	0.542763	SUCCESS
Non Overlapping Template	0.985	0.861716	SUCCESS
Overlapping Template	0.992	0.307255	SUCCESS
Universal	0.987	0.105679	SUCCESS
Approximate Entropy	0.988	0.859647	SUCCESS
Random Excursions	0.990	0.143682	SUCCESS
Random Excursions Variant	0.984	0.930139	SUCCESS
Linear Complexity	0.986	0.068655	SUCCESS
Serial	0.983	0.409792	SUCCESS

As a general remark, one can observe that all binary sequences generated by the proposed dynamical system are random with respect to all tests of NIST suite.

4. CONCLUSIONS

The most used chaotic map in design of chaos based cryptosystem, such as logistic map, tent map, Hénon map etc., have a small space of parameter control for which chaotic behaviour is ensured. In order to ameliorate this shortcoming, we proposed a new dynamical system based on transcendental equation. The chaotic behaviour is ensured for a large space of parameter's values. Its good cryptographic properties are proved using some specific tools from chaos theory, such as Lyapunov exponent, bifurcation diagram and attractor. In addition, we present the results of the standard NIST randomness test applied to binary sequences generated using the proposed map. The very good results obtained prove the good cryptographic qualities of the proposed map, recommending it for using in cryptographic applications both as key-streams generator or as stand-alone pseudorandom number generator.

5. REFERENCES

[1]. Shannon, C., "*Communication theory of secrecy systems*", The Bell System Technical Journal, 28, 656–715, 1949.
[2]. Şerbănescu, A., Rîncu, C.I., "*Systèmes et signaux face au chaos. Applications aux communications*", Military Technical Academy Press, 2008.
[3]. Amigó, J.M., Kocarev, L., Szczepanski, J., "*Theory and Practice of Chaotic Cryptography*", Physics Letters A, 366(3), 211 – 216, 2007.
[4]. Luca, A., Ilyas, A., Vlad, A., "*Generating random binary sequences using tent map*", in Proceedings of the 10th International Symposium on Signals, Circuits and Systems (ISSCS'11), 1-4, Iaşi, Romania, 2011.
[5]. Pareek, N.K., Patidar, V., Sud, K.K., "*A random bit generator using chaotic maps*", International Journal of Network Security, 10(1), 32-38, 2010.
[6]. Zhou, Q., Liao, X., Wong, K.W., Hu, Y., Xiao, D., "*True random number generator based on mouse movement and chaotic hash function*", Information Sciences, 179(19), 3442-3450, 2009.
[7]. Wong, K.W., Kwok, B.S.H., Law, W.S. "*'A fast image encryption scheme based on chaotic standard map"*, Physics Letters A, 372(15), 2645–2652, 2008.
[8]. Kanso, A., Smaoui, N., "*Logistic chaotic maps for binary numbers generation*", Chaos, Solitons & Fractals, 40(5), 2557-2568, 2009.
[9]. Boriga, R., Dăscălescu, A.C., "*A Novel Pseudo-random Bit Generator based on Some Transcendental Chaotic Systems"*, Annals of the Ovidius University - Economic Sciences Series, 11, 208-212, 2011.
[10]. Dăscălescu, A.C., Boriga, R., "*A Novel Fast Chaos-Based Method for Generating Random Permutations with High Shift Factor Suitable for Image Scrambling*", Nonlinear Dynamics, 74(1-2), 307-318, 2013.
[11]. Dăscălescu, A.C., Boriga, R., Diaconu, A.V., "*Study of a New Chaotic Dynamical System and its Usage in a Novel Pseudorandom Bit Generator"*, Mathematical Problems in Engineering, 2013, article ID: 769108, 10 pages, 2013.
[12]. Dăscălescu, A.C., Boriga, R., Răcuciu, C., "*A New Pseudorandom Bit Generator using Compounded Chaotic Tent Maps*", Proceedings of the 9th International Conference on Communications (COMM 2012), Bucharest, Romania, 339-342, 2012.
[13]. Patidar, V., Pareek, N.K., Sud, K.K., "*A Pseudo Random Bit Generator based on Chaotic Logistic*

Map and its Statistical Testing", Informatica, 33, 441–452, 2009.
[14]. Yang, H., Lia, X., Wong, K.W., Zhang, W., Wei, P., "*A new cryptosystem based on chaotic map and operations algebraic"*, Chaos, Solitons and Fractals, 40(5), 2520–2531, 2009.
[15]. Luca, A., Vlad, A., Badea, B., Frunzete, M., „*A study on statistical independence in the tent map"*, IEEE Proceedings of the International Symposium on Signals, Circuits and Systems (ISSCS 2009), Iaşi, Romania, 1–4, 2009.
[16]. Huang, F., Guan, Z.H. "*Cryptosystem using chaotic keys*", Chaos, Solitons and Fractals, 23(3), 851–855, 2005.
[17]. Arroyo, D., Alvarez, G., Li, S., Li, C., Nunez, J., "*Cryptanalysis of a Discrete-Time Synchronous Chaotic Encryption System"*, Physics Letters A, 372(7), 1034–1039, 2008.
[18]. Li, C., Li, S., Alvarez, G., Chen, G., Lo, K.T., "*Cryptanalysis of Two Chaotic Encryption Schemes Base on Circular Bit Shift and XOR Operations*", Physics Letters A, 369, 23–30, 2007.
[19]. Alvarez, G., Montoya, F., Romera, M., Pastor, G., "*Cryptanalysis of an Ergodic Chaotic Cipher"*, Physics Letters A, 311(2-3), 172–179, 2003.
[20]. Alvarez, G., Montoya, F., Romera, M., Pastor, G., "*Cryptanalyzing a Discrete-time Chaos Synchronization Secure Communication System*", Chaos, Solitons and Fractals, 21(3), 689-694, 2004.
[21]. Rukhin, A., Soto, J., Nechvatal, J., Smid, M., Barker, E., Leigh, S., Levenson, M., Vangel, M., Banks, D., Heckert, A., Dray, J., Vo, S., "*A statistical test suite for the validation of random number generators and pseudorandom number generators for cryptographic applications*", NIST Special 800-22, 2010.
[22]. Alligood, K.T., Sauer, T.D., Yorke, J.A., "*Chaos: An Introduction to Dynamical Systems*", Springer Verlag, 1996.
[23]. Wolf, A., Swift, J.B., Swinney, H.L., Vastano, J.A., "*Determining Lyapunov exponents from a time series*", Physica D, 16, 285-317, 1985.
[24]. Farmer, J.D., Ott, E., Yorke, J.A., "*The dimension of chaotic attractors*", Physica D, 7(1-3), 153-180, 1983.
[25]. Grassberger, P., Procaccia, I., "*Measuring the strangeness of strange attractors*", Physica D, 9(1-2), 189-208, 1983.
[26]. Theiler, J., "*Efficient algorithm for estimating the correlation dimension from a set of discrete points*", Physical Review A, 36(9), 4456-4462, 1987.
[27]. Theiler, J., "*Estimating fractal dimension*", Journal of the Optical Society of America, A(7), 1055-1079, 1990.