

# Chaotic Equations Initial Conditions Analysis for Cryptography Applications.

Élvio Dutra<sup>[a]</sup>, Weiler A. Finamore<sup>[b]</sup>, Manfred Glesner<sup>[a]</sup>, Leandro Indrusiak<sup>[c]</sup>, Peter Zipt<sup>[a]</sup>.

**Resumo**—Nesta última década, muitos artigos em que equações caóticas são usadas como a ideia central em algoritmos criptográficos surgiram. Embora muitos destes algoritmos usem as Condições Iniciais (IC) de equações diferenciais caóticas como chave criptográfica, um estudo preciso das ICs válidas (aquelas que conduzem ao caos) não foi realizado. Neste artigo, é analisada a equação diferencial caótica mais elementar, descoberta por Linz e Sprott, com o objetivo de determinar  $V_{IC}$  (a região de Condições Iniciais Válidas) e a sua importância na determinação do espaço de chaves para algoritmos criptográficos baseados em caos.

**Palavras-Chave**—Caos, criptografia, fluxo caótico, condições iniciais, atrator, espaço de chaves criptográficas.

**Abstract**—In the last decade, many articles appeared which apply chaotic equations as the core of encryption algorithms. Although many of these algorithm use the Initial Conditions (IC) of chaotic differential equations as secret key, a precise study of the Valid ICs (those leading the behavior of the equation to chaos) has not being made. In this paper we analyze the most elementary piecewise linear chaotic flow, proposed by Linz and Sprott, with focus on the determination of the  $V_{IC}$  (the region of Valid Initial Conditions) and its influence in determining the key space of chaos-based encryption algorithms.

**Keywords**—chaos, encryption, jerk, piecewise linear chaotic flow, initial conditions, attractor, key space.

## I. INTRODUCTION

Lorenz 1963 seminal article [1] started chaos theory and its application to many disciplines, including mathematics, mechanics, biology, ecology, astronomy, telecommunications and cryptology. Since Lorenz, more than twenty differential equations systems with chaotic behavior have being reported [4], [5], [6], [26]. Chaos and Encryption are intimately tied [27], [28] — *confusion* and *diffusion* are properties strongly related to the chaotic properties of *ergodicity* and *sensitivity to initial conditions* [29]. This relation lead many researchers to develop chaos based encryption algorithms: Baptista [12] algorithm, by mapping plain text to the number of iterations performed on the Chaotic Logistic Equation [12] to move the cipher key dependent chaotic attractor's (or path) initial state (or initial condition, IC)  $x_0$ , to a final state related to the plain text; the cipher text in the scheme by Alvarez et al [13] is a triplet composed by  $x_0$ , a given threshold  $U$  and a parameter  $B$  used by the transmitter to locate the plain text on a binary chain  $C$  constructed according to the threshold  $U$ . In

[14] Jakimoski and Kocarev proposed a procedure to create chaos ciphers and Wong, [15], improves Baptista [12] cipher by dynamically updating the look-up table that assigns plain text to the corresponding attractor regions. Wong's cipher was further improved by methods which use control parameters and hashing schemes [16], [17], [20], [21] and in [30] Li et all proposed a real-time scheme that applies a cascade of chaotic maps, mixing stream and block cipher techniques.

The chaotic differential equation's behavior is very sensitive to IC variations — a known fact, from the nonlinear dynamics, is that this chaotic behavior even disappears for certain IC. The Key Space, a factor responsible for the strength of the encryption scheme, is determined by the size of the set of valid IC that drives the system to chaos. The motivation behind this study is the characterization of the region of IC values that renders a chaotic system behavior — we will use the notation  $V_{IC}$  when referring to the set of valid IC's.

This paper is organized as follows: Section II presents the elementary, piecewise linear, chaotic equation discovered by Linz and Sprott [11], which will be used as study case in this article. Section III characterizes the region of  $V_{IC}$ , with respect to the three-dimensional chaotic attractor of Linz and Sprott. Section IV presents a practical example of key space calculation for a given chaos-based encryption algorithm. Section V presents the conclusions.

## II. LINZ AND SPROTT ELEMENTARY SYSTEM

As the result of extensive numerical search, Linz and Sprott [11] found the simplest known non-polynomial, autonomous, three-dimensional, dynamical system that exhibits chaos. Equation (1), describing the system, is a piecewise linear chaotic dynamics that contains only one control parameter  $A$ , and only one nonlinearity.

$$x''' + Ax'' + x' + |x| - 1 = 0 \quad (1)$$

Equation (1) can also be written in the form

$$\begin{cases} x' = y \\ y' = z \\ z' = -Az - y - |x| + 1. \end{cases} \quad (2)$$

<sup>[a]</sup>Institute of Microelectronics Systems, Technische Universität Darmstadt, Germany, <sup>[b]</sup>Centro de Estudos em Telecomunicações da PUC-Rio, Pontifícia Universidade Católica do Rio de Janeiro, Brazil, <sup>[c]</sup>Department of Computer Science, The University of York, United Kingdom. E-mails: elvio@ciscea.gov.br, weiler@cetuc.puc-rio.br.

The selection of this chaotic equation as case study, relies on the fact that it has simple expression and it yields to a low complexity hardware implementation [5], [10]. Fig. 1 displays a top view of the chaotic attractor for  $A = 0.6$ ,  $\mathbf{x}_0 = (x_0, y_0, z_0) = (0, 0, 0)$  in Equation (1). Although Linz

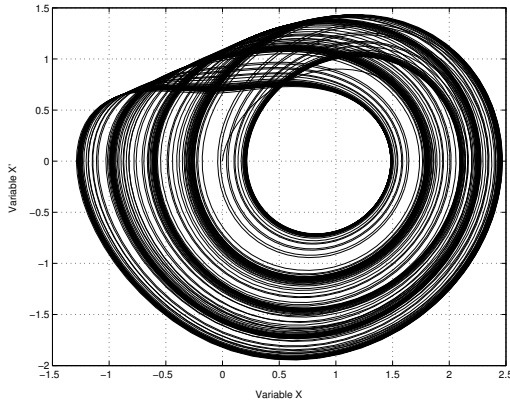


Fig. 1. Top view of the chaotic attractor of Linz and Sprott's equation obtained with  $A = 0.6$  and  $(x_0, y_0, z_0) = (0, 0, 0)$ .

and Sprott precisely characterizes, on their work, the range of values of the parameter  $A$ , which yields the system to chaos, the characterization of the region  $V_{IC}$ , which is the subject of the present work, is missing.

### III. VALID INITIAL CONDITIONS REGION

This chapter has two related purposes: (i) to show how to determine if a given  $IC$  leads the dynamical of Linz and Sprott's Equation (1) to a chaotic or non-chaotic behavior and (ii) to characterize (by simulation) the region of all valid  $IC$  of Linz and Sprott's chaotic equation.

It is worth mentioning that all chaotic flows have inherently the following characteristics: determinism, sensitive dependence on  $IC$ , non-periodicity, and "stability" with some tension and boundedness. From a mathematical perspective, chaos orbits do not have to be bounded. From a practical point-of-view, however, stability is so important that it is better to impose stability constraints such that chaos motion of the chaotic attractor is locally unstable but globally it is stable. As such, chaos can be seen as a bounded phenomenon, involving a kind of loose stability. Fig.1 illustrates a bounded chaotic attractor with the variable  $x$  restricted to the interval  $(-1.29, 2.47)$  and the variable  $y$  restricted to the interval  $(-1.95, 1.43)$ . The chaotic attractor set, say  $\mathcal{A}$ , is a three-dimensional set of points with values of  $z$  in the range  $(-1.83, +1.53)$ , as sketched on Fig. 2.

The trajectories of states of Equation (1), or paths, depend on the  $IC$  used, and can constitute a chaotic attractor like the paths exhibited on Fig. 1 and Fig. 2, or exhibit a non-chaotic behavior. The paths generated by a chaotic equation, can be classified, for purposes, in one of the three categories listed

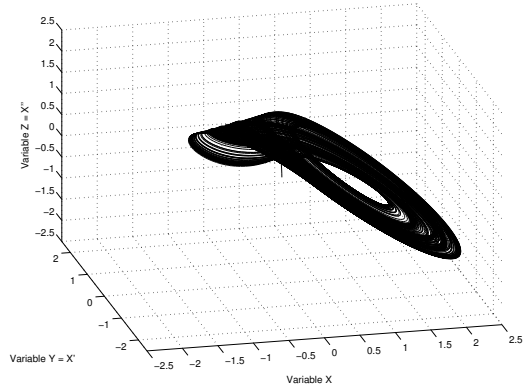


Fig. 2. Three-dimensional chaotic attractor for  $\mathbf{x}_0 = (0,0,0)$ .

next, revealing a system with a non-chaotic behavior.

- 1) **[Convergency]** The three-dimensional attractor converges to an specific point;
- 2) **[Cyclicity]** The three-dimensional attractor cycles indefinitely;
- 3) **[Divergency]** The three-dimensional attractor diverges to plus or minus infinity;

The non-chaotically behavior verification was performed by examining the final states of the simulated equation as well as examining the maximum Lyapunov Exponent. This exponent was obtained with the algorithm proposed by Wolf et al [32], considering that the Equation (1) has a single independent term.

In the selected study case, except for two non-chaotic convergent points,  $(1, 0, 0)$  and  $(-1, 0, 0)$ , that correspond to poles of Equation (1), all non-valid  $IC$ 's drive the system to divergency.

It should be noticed that all states belonging to a chaotic attractor also belong to  $V_{IC}$ . Furthermore, the path  $\tau_i$  having as origin an  $IC$  point belonging to a given path  $\tau_j$  belonging to the attractor will coincide from this  $IC$  point on, with the path  $\tau_j$ . The reason for this behavior relies on the fact that, like in a Markov Chain, the next state is only dependent on the current state.

This property leads us to the conclusion that the region  $V_{IC}$  minimally contains all points of the three-dimensional chaotic attractor (as pointed out later, this region contains the three-dimensional chaotic attractor). This situation is summarized on Table I where  $x_{min}$  and  $x_{max}$  represent the minimum and maximum values obtained while simulating Equation (1). The same notation is applied with respect to the other dimensions variables  $y$  and  $z$ .

What has been shown quantitatively on Table I, is qualitatively exhibited on Fig. 3 — that shows, three-dimensionally, the volume  $V_{IC}$  printed in shades of color with the chaotic attractor printed in black on the bottom part of Fig. 3.

TABLE I  
LIMITS OF THE KEY SET (PARALLELEPIPED) IMBEDDED IN  $V_{IC}$ .

	$x_{min}$	$x_{max}$	$y_{min}$	$y_{max}$	$z_{min}$	$z_{max}$
Attractor	-1.29	2.47	-1.95	1.43	-1.83	1.53
Valid $IC$	-6.50	39.5	-33.5	4.50	-3.19	30.2

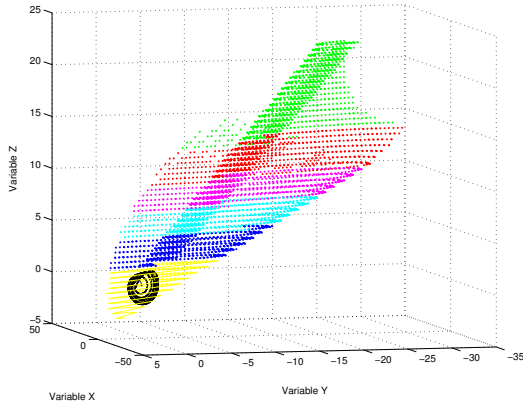


Fig. 3. Three-dimensional chaotic attractor immersed in region  $V_{IC}$ .

Points in Fig. 4 correspond to the intersection of the 3-D region  $V_{IC}$ , shown in Fig. 3, and the plane  $z = 0$ . The large, outer, red area surrounding the green area corresponds to non-valid diverging  $IC$  ( $\bar{V}_{dIC}$ ). The green inner area surrounded by  $\bar{V}_{dIC}$  corresponds to the  $V_{IC}$  in this plane  $z = 0$ . Also shown in this figure, are two non-valid converging  $IC$ 's, marked by a red circle, namely points  $(1, 0, 0)$  and  $(-1, 0, 0)$ . All points in the red area enclosed by the green area are  $IC$  points that drive Equation (1) to a diverging, non-chaotic trajectories, which loop around the attractor once before diverging to minus infinity.

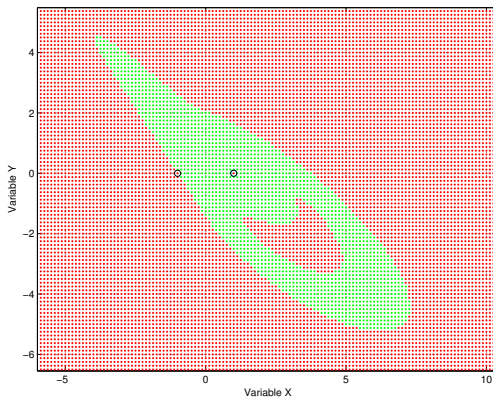


Fig. 4. Intersection of the 3-D region  $V_{IC}$  with the plane  $z = 0$ .

Fig. 5 is an enlargement of Fig. 4 which, besides displaying the chaotic attractor, also shows the intersection of  $\mathcal{A}$  with the plane  $z = 0$ . The black points highlight these intersections. One can see, by examining this picture, that the green area  $V_{IC}$  contains the attractor (points displayed in black), corroborating an statement made before on this section.

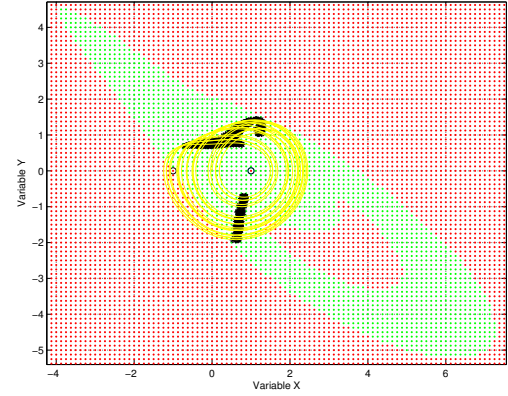


Fig. 5. Intersection of the 3-D Attractor and plane  $z = 0$ , and the intersection of  $V_{IC}$  and plane  $z = 0$

#### IV. KEY SPACE CALCULATION

We will now consider the algorithm proposed by Baptista [12] to determine the key space  $\mathcal{K}$  and its relation to  $V_{IC}$ . Let the string  $(a_1, a_2, \dots, a_S)$  be the plain text to be encrypted. The chaotic equation used in [12] is the so called Logistic Equation — we replaced this, in our study, by the Linz and Sprott equation (1). Given an initial condition  $x_0$ , a partition  $\mathcal{L} = \{\mathcal{L}_1, \mathcal{L}_2, \dots, \mathcal{L}_S\}$  of the chaotic attractor  $\mathcal{A}$ , Baptista algorithm associates each letter  $a_i$  from the plain text to a curve  $\mathcal{L}_i$  and the cipher text  $c_i$  is made equal to  $\ell_i \in \mathbb{N}$ , the integer number of iterations required to drive the state of the system from  $x_0$  to state  $x_i \in \mathcal{L}_i$ . The secret key  $k = (A, x_0, \mathcal{L}) \in \mathcal{K}$  is then a triplet formed by the parameter of Linz and Sprott's Equation  $A$ , the  $IC$   $x_0$  and, the partition  $\mathcal{L}$ .

The next two figures present two slices of the three-dimensional region  $V_{IC}$  at  $z = -2.0$  (Fig. 6) and  $z = -1.5$  (Fig. 7). The intersection of  $V_{IC}$  and the two planes delimit two large and connected parallelepiped sets arbitrarily chosen based on the values shown on Table II — as before notice that  $x_{min}$ ,  $x_{max}$ ,  $y_{min}$ ,  $y_{max}$ ,  $z_{min}$  and  $z_{max}$  are the limits of a parallelepiped belonging to the green 3-D region presented on Fig. 6 and Fig. 7.

TABLE II  
LIMITS OF THE KEY SET (PARALLELEPIPED) IMBEDDED IN  $V_{IC}$ .

$x_{min}$	$x_{max}$	$y_{min}$	$y_{max}$	$z_{min}$	$z_{max}$
0.500	1.500	-0.125	1.375	-2.000	-1.500

The cardinality of the key set depends, of course, on the arithmetic precision ( $\delta$ ) and on the number of iterations ( $\eta$ ) — usually a large number is necessary to uncorrelate the initial and final state. The trade-off between key space size and encryption speed has, as always, to be considered. To qualitatively illustrate the influence of the number of iterations

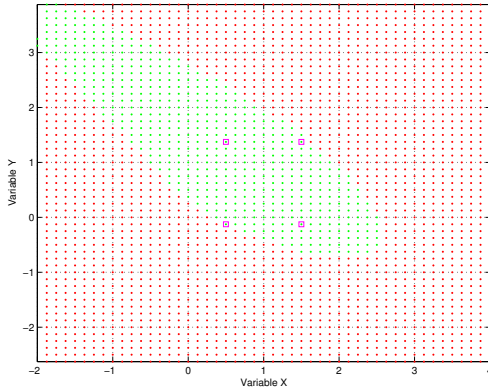


Fig. 6. Slice of the 3-D valid-*IC* Region, at  $z = -2.0$ , where the lower frontier of the Key Space set lies.

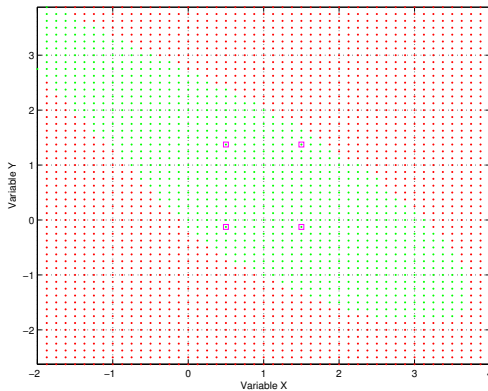


Fig. 7. Slice of the 3-D valid-*IC* Region, at  $z = -1.5$ , where the upper frontier of the Key Space set lies.

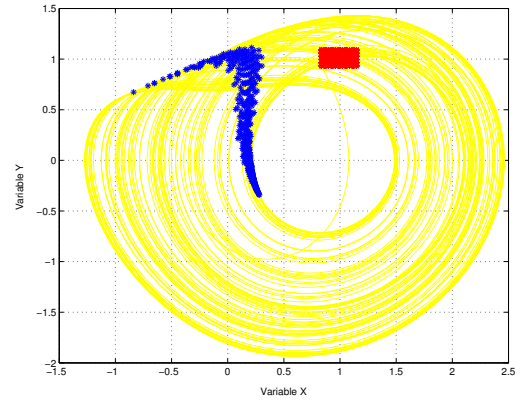


Fig. 8. Volumetric dispersion ( $3.95 \times 10^{-2}$ ) of final states of Linz and Sprott's equation after 30 iterations ( $\delta = 2^{-5}$ ).

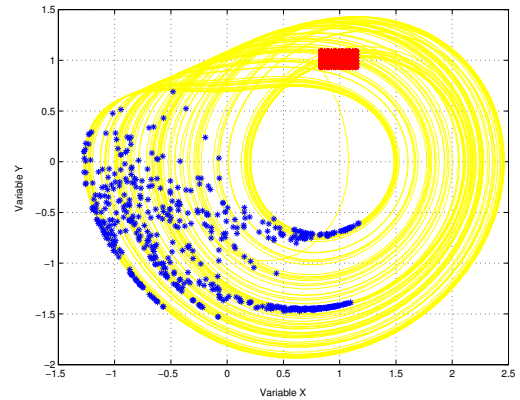


Fig. 9. Volumetric dispersion ( $1.71 \times 10^{-1}$ ) of final states of Linz and Sprott's equation after 100 iterations ( $\delta = 2^{-5}$ ).

on the correlation between states, Fig. 8 to Fig. 11 display the dispersion observed among states. The red rectangle centered on (1.0, 1.0) is a cluster of 594 points, each point separated from its nearest neighbor, by a distance of  $2^{-5}$ . Each one of these 594 red points, when used as *IC*, produces one of the 594 final states displayed in blue on Fig. 8 which depicts the simulation results after 30 iterations — notice the 594 final states are grouped on the second quadrant (*V*-shaped set). The volumetric dispersion (measured by the multiplication of the standard deviation, along dimensions  $x$ ,  $y$  and  $z$ ) of these final states is small, approximately  $3.95 \times 10^{-2}$ .

The dispersion of equivalent set of points after 100 and 500 iterations are shown on Fig. 9 and Fig. 10. Now the final internal states (594 blue points) experimented volumetric dispersions near  $1.71 \times 10^{-1}$  and  $5.08 \times 10^{-1}$ , respectively. Finally, Fig. 11 presents the same information after 1100 iterations, when the final states are spread all over the chaotic attractor (the volumetric dispersion is about  $8.28 \times 10^{-1}$ ).

From the graph of the volumetric dispersion depicted as a function of the number of iterations, on Fig. 12 one can see that, after a large enough number of iterations, the final internal states are scattered all over the chaotic attractor volume.

When the selected precision grows higher, the *IC* points are closer to each other and a larger number of iteration is

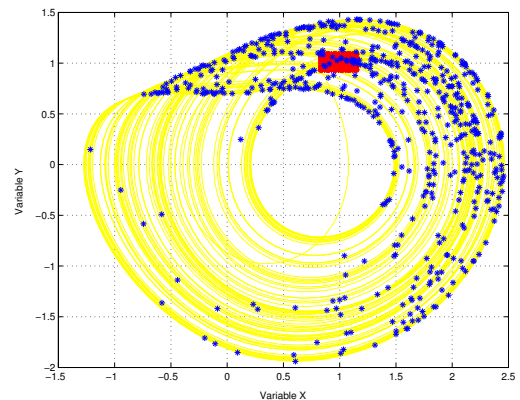


Fig. 10. Volumetric dispersion ( $5.08 \times 10^{-1}$ ) of final states of Linz and Sprott's equation after 500 iterations ( $\delta = 2^{-5}$ ).

required to ensure that the dispersion is large enough. Fig. 13 exhibits the volumetric dispersion, for three different precision values:  $\delta = 2^{-20}$  (red cycles),  $\delta = 2^{-30}$  (blue diamonds) and  $\delta = 2^{-40}$  (green squares). The values of volumetric dispersion, after, respectively,  $\eta = 290$ ,  $\eta = 430$  and  $\eta = 505$  iterations, start to increase rapidly, as shown.

Chaotic equations are very sensitive to variations on the



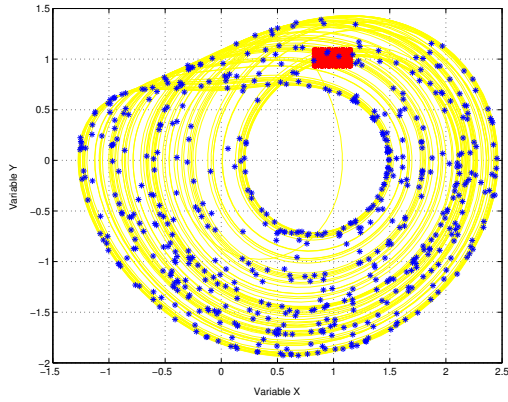


Fig. 11. Volumetric dispersion ( $8.28 \times 10^{-1}$ ) of final states of Linz and Sprott's equation after 1100 iterations ( $\delta = 2^{-5}$ ).

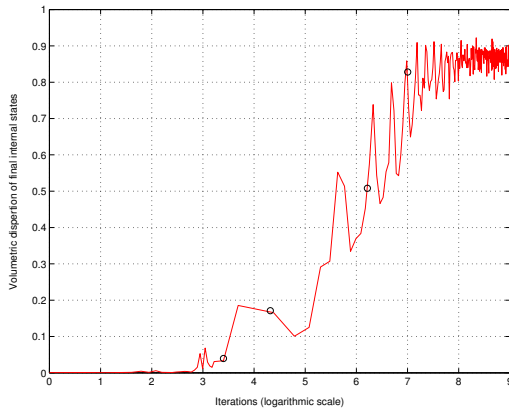


Fig. 12. Volumetric dispersion of final states of Linz and Sprott's equation, versus number of iterations (in natural logarithmic scale) ( $\delta = 2^{-5}$ ).

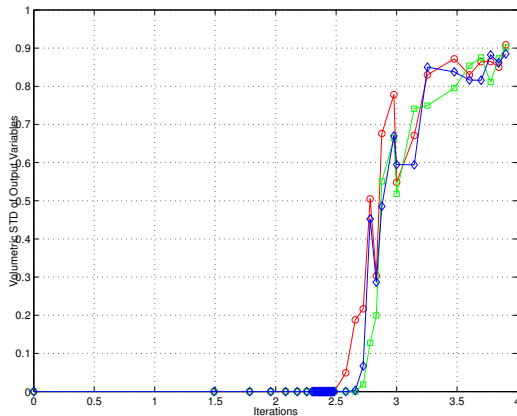


Fig. 13. Time evolution (in logarithmic scale) of the volumetric dispersion of the final states, of Linz and Sprott's equation.  $\delta = 2^{-20}$  (red cycles),  $\delta = 2^{-30}$  (blue diamonds) and,  $\delta = 2^{-40}$  (green squares).

value of the *IC*'s — a slight change on *IC*,  $\delta = 2^{-40}$  for instance, drives the final states, in a butterfly effect<sup>1</sup> [33]

<sup>1</sup>“The flapping of a single butterfly's wing today produces a tiny change in the state of the atmosphere. Over a period of time, what the atmosphere actually does, diverges from what it would have done. So, in a month's time, a tornado that would have devastated the Indonesian coast doesn't happen. Or maybe one that wasn't going to happen, does.”

manner, to a large dispersion, as Figs.12 and 13 illustrate.

The graphic of the dispersion as a function of the variation of *IC*'s of the chaotic Linz and Sprott equation displayed on Fig. 14 is also an evidence of this sensitivity. This graph plots the distances between every *IC* state and the correspondent final state, after iterating the chaotic equation 1815 times — minimum distance between distinct *IC*'s (precision) is set to  $\delta = 2^{-40}$ .

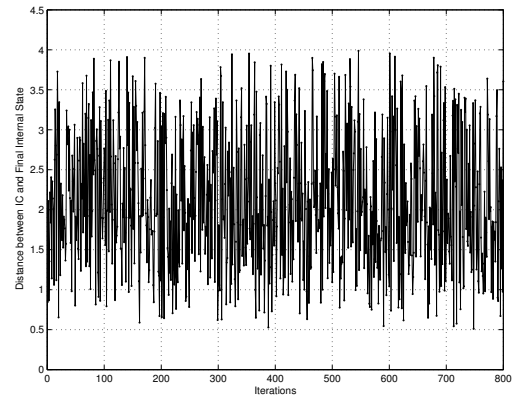


Fig. 14. Variation of the distances between the *IC* state  $x_0 = (0.25, -0.375, 1.5)$  and the correspondent final state,  $x_\eta$ , after  $\eta = 1815$  iterations ( $\delta = 2^{-40}$ ).

The dispersion of the final states of the chaotic equations when distinct *IC* are used can guide the choice for the number of iterations. The plots of number of iterations versus minimum distance between *IC* to achieve volumetric dispersions of 0.5 (square marks), 0.7 (circle marks) and 0.8 (diamond marks), is displayed on Fig. 15. A good

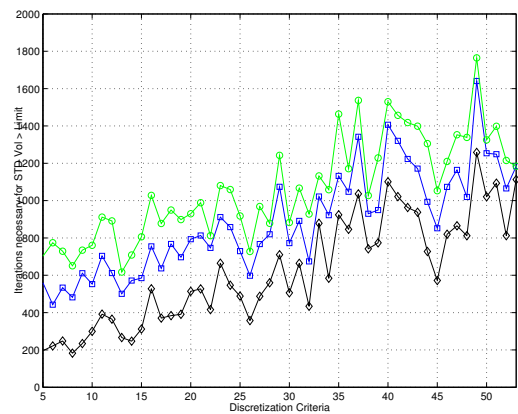


Fig. 15. Number of iterations necessary to disperse the final internal states over the chaotic attractor as function of the distance between successive Initial Conditions.

trade-off between the number of iterations and the minimum distance between *IC* is observed, from the results on Fig. 15, to be  $\eta = 1053$  and  $\delta = 2^{-45}$ . With this choice of parameters a key set with cardinality  $\times 2^{135}$  or, equivalently, 135 bits long key can be constructed.

If we use the whole volume of the attractor of Fig. 15, instead of only the volume of the parallelepiped specified by Table II, the key set can reach a cardinality of, roughly,  $2^{150}$  or, equivalently, a 150 bits long key.

## V. CONCLUSIONS

In this paper, a characterization of the three-dimensional region of Initial Conditions that leads the elementary chaotic flow, discovered by Linz and Sprott, to a chaotic attractor is presented, delimiting thus a spatial region with  $IC$  suitable for use with encryption algorithms. A simple analysis has shown how to obtain a key set with keys of 135 bits long (this number can be even large if parameters other than the binary representation of the chaotic equation solution are used). Further work, under way, seek to characterize the valid  $IC$  region in three-dimensional regions, for other commonly used chaotic equation.

## REFERÊNCIAS

- [1] Lorenz, N. Edward, *Deterministic non-periodic flows*. Journal of Atmospheric Science, Vol. 22, No 02, 1963
- [2] Madan, Rabinder N.: *Chua's Circuit: A Paradigm for Chaos*. World Scientific Series on Nonlinear Science, Series B, Vol. 1, ISBN 981-02-1366-2.
- [3] Chan, Kung-Sik and Tong, Howel: *Chaos: A Statistical Perspective*. Springer Series in Statistics, 2001.
- [4] Rössler, O. E.: An equation for continuous chaos, Physics Letter 35A, 1976.
- [5] Sprott, J. C., Linz, S. J.: Algebraically simple chaotic flows. International Journal of Chaos Theory and Applications, 2000, Vol. 5, No. 2.
- [6] Sprott, J. C.: Some simple chaotic flows. Physical Review E, 1994, Vol. 50, Nr. 2, R647.
- [7] Sprott, J. C.: *Chaotic Attractors: Creating Patterns in Chaos*. M&T Books, ISBN 1-55851-298-5.
- [8] Bartissol, P. and Chua, L. O.: The Double Hook. IEEE Transactions on Circuits and Systems, Vol. 35, Nr. 12, December 1988.
- [9] Sobhy, M. I.: Secure Computer Communication Using Chaotic Algorithms. International Journal of Bifurcation and Chaos, Vol. 10, Nr. 12, March 2000.
- [10] Sprott, J. C.: A New Class of Chaotic Circuit. Physics Letters, A 266 (2000) 19 - 23, 14th February 2000.
- [11] Linz, S. J., Sprott, J. C.: Elementary Chaotic Flow. Physics Letters, A 259 (1999) 240 - 245, 16th August 1999.
- [12] Baptista, M. S.: Cryptography with chaos. Physics Letters, A 240 (1998) 50 - 54.
- [13] Alvarez, E., Fernandez, A., Garcia, P., Jimenez, J., Marcano, A.: New approach to chaotic encryption. Physics Letters, A 263 (1999) 373 - 375.
- [14] Jakimoski, G., Kocarev, L.: Chaos and cryptography: Block encryption ciphers based on chaotic maps. IEEE Transactions on Circuits and Systems, Vol. 48, Nr 2, 2001.
- [15] Wong, K. W.: A fast chaotic cryptographic scheme with dynamic look-up table. Physics Letters, A 298 (2002) 238 - 242.
- [16] Wong, K. W., Ho, S. W., Yung, C. K.: A chaotic cryptography scheme for generating short ciphertext. Physics Letters, A 310 (2003) 67 - 73.
- [17] Wong, K. W.: A combined chaotic cryptographic and hashing scheme. Physics Letters, A 307 (2003) 292 - 298.
- [18] Alvarez, G., Montoya, F., Romera, M., Pastor, G.: Cryptanalysis of an ergodic chaotic cipher. Physics Letters, A 311 (2003) 172 - 179.
- [19] Alvarez, G., Montoya, F., Romera, M., Pastor, G.: Cryptanalysis of dynamic look-up table based chaotic cryptosystems. Physics Letters, A 326 (2004) 211 - 218.
- [20] Xiao, D., Liao, X., Wong, K. W.: Improving the security of a dynamic look-up table based chaotic cryptosystem. IEEE Transactions on Circuits and Systems, Vol. 53, Nr 6, 2006.
- [21] Xiang, T., Liao, X., Tang, G., Ghen, Y., Wong, K. W.: A novel block cryptosystem based on iterating a chaotic map. Physics Letters, A 349 (2006) 109 - 115.
- [22] Wang, Y., Liao, X., Xiang, T., Wong, K. W., Yang, D.: Cryptanalysis and improvement on a block cryptosystem based on chaotic. Physics Letters, A 363 (2007) 277 - 281.
- [23] Li, Z., Li, K., Wen, C., Soh, Y. C.: A new Chaotic Secure Communication System. IEEE Transaction on Communication, Vol 51, Nr. 8, August 2003.
- [24] Li, S., Chen, G., Wong, K. W., Mou, X., Cai, Y.: Baptista Type Chaotic Cryptosystems - Problems and Countermeasures. Physics Letters, A 332 (2004) 368 - 375.
- [25] Behnia, S., Akhshani, A., Ahadpour, S., Mahmodi, H., Akhavan, A.: A fast chaotic encryption scheme based on piecewise nonlinear chaotic maps. Physics Letters, A 366 (2007) 391 - 396.
- [26] Chua, L. O.: The genesis of Chua's circuit. Archiv fur Elektronik und Uebertragungstechnik, Vol. 46, Nr. 04, July 1992.
- [27] Shannon, C. E., A mathematical theory of communication. Bell System Technical Journal, vol. 27, pp. 379-423 and 623-656, 1948.
- [28] Shannon, C. E., Communication theory of secrecy systems. Bell System Technical Journal, vol. 28, pp. 656-715, 1949.
- [29] Alvarez, G., Li, S.: Some Basic Cryptographic Requirements for Chaos-Based Cryptosystems. International Journal of Bifurcation and Chaos, Vol. 16, Nr. 08, 2129 - 2151, 2006.
- [30] Li, S., Zheng, X., Mou, X., Cai, Y.: Chaotic Encryption Scheme for Real-Time Digital Video. Proceedings of SPIE, Vol. 4666, pp. 149 - 160, 2002.
- [31] Ataei, M., Khaki-Sedigh, A., Lohmann, B., Lucas, C.: Estimating the Lyapunov Exponents of Chaotic Time Series: A Model Based Method.
- [32] Wolf, A., Swift, J. B., Swinney, H. L. Vastano, J. A.: Determining Lyapunov Exponents from a time series. Physica D, 16, pp. 285 - 317, 1985.
- [33] I. Stewart, *Does God Play Dice? The New Mathematics of Chaos*, Penguin Books, London, England, p.129, Second Edition, 1996.