A BASIC FRAMEWORK FOR THE CRYPTANALYSIS OF DIGITAL CHAOS-BASED CRYPTOGRAPHY

David Arroyo[1], *Gonzalo Alvarez*[1] *and Veronica Fernandez*[1]

[1]Instituto de Física Aplicada, Consejo Superior de Investigaciones Científicas,
Serrano 144—28006 Madrid, Spain

ABSTRACT

Chaotic cryptography is based on the properties of chaos as source of entropy. Many different schemes have been proposed to take advantage of those properties and to design new strategies to encrypt information. However, the right and efficient use of chaos in the context of cryptography requires a thorough knowledge about the dynamics of the selected chaotic system. Indeed, if the final encryption system reveals enough information about the underlying chaotic system it could be possible for a cryptanalyst to get the key, part of the key or some information somehow equivalent to the key just analyzing those dynamical properties leaked by the cryptosystem. This paper shows what those dynamical properties are and how a cryptanalyst can use them to prove the inadequacy of an encryption system for the secure exchange of information. This study is performed through the introduction of a series of mathematical tools which should be the basic framework of cryptanalysis in the context of digital chaos-based cryptography.

Index Terms— chaos, cryptography, entropy, wavelet transforms

1. INTRODUCTION

Chaotic cryptography has been an important research area during the last two decades. The properties of chaotic systems have been used in very different ways to build new cryptosystems. All of those proposals can be classified into two big families, which are analog chaos-based cryptosystems and digital chaos-based cryptosystems. The first type of chaotic cryptosystems is based on the chaotic synchronization technique [1], whereas digital chaotic cryptosystems are designed for digital computers. The scope of this paper is related to the last type of chaotic cryptosystems. Since the performance and accuracy of digital chaotic cryptosytems is a translation of the dynamical properties of the underlying dynamical system, the first step in either their design or their analysis comes from the evaluation of those properties. This assessment has as main goal the verification that the selected dynamical system evolves in a chaotic way in the context defined by the encryption strategy. Furthermore, it must be confirmed the impossibility of guessing the key or part of the key by the examination of that chaotic behavior. Indeed, chaotic systems exhibit an underlying regularity which could represent a problem in the context of chaotic cryptography. The present work presents a set of mathematical tools for the analysis of the dynamical properties of chaotic systems and, consequently, for the detection of design problems in digital chaos-based cryptosystems. More specifically, this work studies the relationship between the set defined by the initial conditions and the control parameter of chaotic systems and their temporal evolution. From the point of view of the security concerns of cryptography, this work is a first step to establish a paradigm of requirements for the adequate association of chaotic systems and encryption architectures.

2. CHAOS AND CRYPTOGRAPHY

The use of chaotic systems in cryptography is motivated by the similarity between the needs of cryptography and the main characteristics of chaos. Indeed, every *cryptosystem*, i.e., every encryption system performs the transformation of an input (the *plaintext*) into an output (the *ciphertext* or *cryptogram*) in such a way that the different inputs and outputs of the systems are statistically independent. Moreover, this transformation depends on an external parameter called *key* of the cryptosystem. If a cryptosystem has been designed in a correct way, then its output is statically independent from the key and from the input. In other words, a good cryptoystem shows *diffusion* and *confusion* properties [2]. The confusion property means that the temporal evolution of the output of the cryptosystem is statistically independent from the input and from the key. Chaotic systems shows an ergodic behavior and, consequently, possess inherently the confusion property with respect to the initial conditions and the control parameter(s). On the other hand, the diffusion property implies that an small change in the input of the cryptosystem is translated into a large modification in the

The work described in this paper was supported by *Ministerio de Educación y Ciencia of Spain*, research grant SEG2004-02418, *Ministerio de Ciencia y Tecnología* of Spain, research grant TSI2007-62657 and *CDTI, Ministerio de Industria, Turismo y Comercio of Spain* in collaboration with Telefónica I+D, Project SEGUR@ with reference CENIT-2007 2004.

output. Chaotic systems are characterized by a high sensitivity to initial conditions and the control parameter(s) and thus chaos can also be used as a source of diffusion. Nevertheless, chaotic systems are sustained by an underlying regularity by means of the existence of dense unstable periodic orbits which further constitute the *skeleton* of chaos [3, p. 413]. Furthermore, chaotic systems generally considered for cryptographic applications are defined in a parametric way and not all the values of the control parameter(s) lead to a chaotic behavior. As a result, the design of a secure and efficient chaos-based cryptosytem requires the selection of an encryption architecture that conceals the underlying regularity of the chosen chaotic system and, at the same time, guarantees that the control parameter(s) used in the encryption and decryption processes are those which drive the dynamical system into a chaotic behavior. Concerning this last point, it is highly recommendable to use dynamical systems with a large and continuous set of values for the control parameter(s) such that evolution in a chaotic way is guaranteed. According to all this considerations, the cryptanalysis work can be only successful when a chaotic cryptosystem leaks too much information about the dynamics of the underlying chaotic system or when the selection of the control parameter(s) is not done conveniently.

3. DETECTION OF NON-CHAOTIC BEHAVIOR

The scope of this paper is digital chaos-based cryptography and thus the next work is focused on dynamical systems defined in discrete time. These dynamical system are also called *maps* and are mathematically defined by a difference equation

$$x_{k+1} = g(\mu, x_k), \tag{1}$$

where $x, g(x) \in U \in \mathbb{R}^n$, being U the phase space, and μ is an array of control parameters in $V \subset \mathbb{R}^p$. This section is concerned with the definition of mathematical tools to decide whether a digital chaotic cryptosystem defines a good framework for the selection of the set of control parameters of the underlying chaotic map.

3.1. Bifurcation diagram

A first method to detect problems related to the definition of the method of selection of values for the array of control parameters is based on the evaluation on the asymptotic temporal evolution. The temporal evolution or *orbit* of a discrete-time dynamical system is determined for a certain initial condition and a certain set of values for the array of control parameters as

$$\gamma(\mu, x_0) = \{x_0, x_1, \ldots, x_n\}. \tag{2}$$

If the considered dynamical system is a chaotic map, then the orbit derived from any initial condition covers the whole phase space. This characteristic can be verified by plotting $\gamma(\mu, x_0)$ for x_0 selected randomly in U and μ taking all the values in V. This representation is called *bifurcation diagram* and can be used to detect values of μ not leading to chaos. As an example, in Fig. 1 the bifurcation diagram for the logistic map is shown identifying those *inadequate* values of μ. When considering a chaotic cryptosystem, the possibility of selecting those values of μ associated to a non-chaotic behavior implies a degradation of the performance of the cryptosystem and can be used by a cryptanalyst [4, 5].

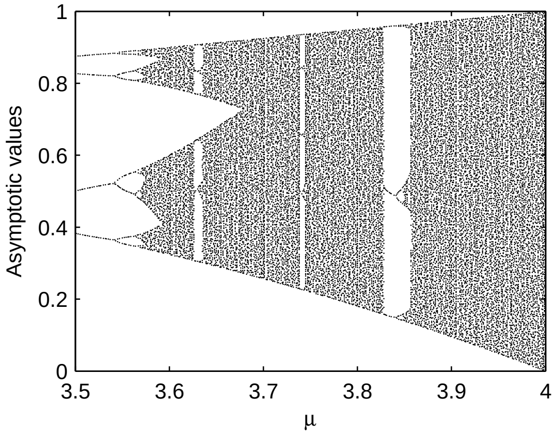


Figure 1. Bifurcation diagram of the logistic map.

3.2. The Lyapunov exponent

One important rule for the design of chaotic cryptosystems is the accurate definition of the key space [6, Rule 5]. Therefore, cryptanalysis is also concerned with the evaluation of the preciseness of the definition of the key space. A very useful tool for this assessment is the Lyapunov exponent or LE. Indeed, the LE quantifies the local divergence of a dynamical system in such a way that a positive value of the LE informs of a chaotic behavior. More rigorously, for a phase space defined in $\mathbb{R}^m$ there exist m Lyapunov exponents and chaos exists when the largest Lyapunov exponent is positive. The Hénon map is a two dimensional dynamical system and the control parameter vector is given by $\mu = [a, b]$. If the Hénon is considered for cryptographic applications, then the encryption architecture must assure that the selection of a and b during the encryption/decryption procedure always guarantees a positive LE (see Fig. 2). Otherwise, a degradation in the performance of the cryptosystem is observed as it occurs in the cryptosytesm analyzed in [7–9]

4. EXPLOITING THE LEAKING OF THE UNDERLYING CHAOTIC SYSTEM REGULARITY

Most chaos-based cryptosystems used either the initial conditions or the control parameter(s) or both as key. Therefore, the security of those proposals is very dependent on the possibility of estimating the control parameter(s) and/or the initial conditions from the information provided by the

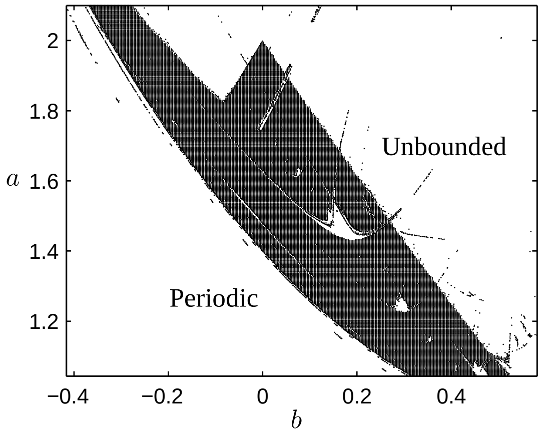


Figure 2. Determination of the chaotic region of the Hénon by means of the Lyapunov exponent.

cryptosystem. The success of this estimation process is something to consider in the design of a new cryptosystem. Indeed, if it is known how much information can be provided to a cryptanalyst without exposing our encryption system, then it is possible to build a secure but also more efficient cryptosystem. The information that can be used by an attacker or cryptanalyst is either part of an orbit or the transformation of part of an orbit of the underlying chaotic system. Actually, that part of an orbit or the transformation of the part is associated to a certain initial condition and control parameter(s) value. Consequently, the cryptanalyst work is focused on looking for one-to-one relationship between those samples of orbits or those transformation of the samples of orbits. Next some mathematical procedures for this estimation task are shown.

4.1. Study of histograms and the return map

In some digital chaos-based cryptosystems the result of the encryption procedure, i.e., the different cryptograms are given directly by the orbit of some chaotic system [10] or by the sampling process on the orbit of a chaotic system [11, 12]. In the first case, the cryptosystem shows a clear security problem, since chaotic maps are defined using a difference equation which implies that two consecutive values of an orbit can be used to estimate the control parameter value [5]. In the second situation, the orbit is sampled and thus it is not possible a direct estimation of the control parameter(s) as before. However, it is possible to associate those sampling values with the control parameter(s) by either the study of the return map or by an statistical treatment. Indeed, according to Kerckhoffs' principle [13, p. 14], the chaotic map used for a certain digital chaos-based cryptosystem is known by anyone and, consequently, a cryptanalyst knows and can study its return map. In [14,15], for example, this study is used to estimate the control parameter of the logistic map by means of the maximum value of its return map. On the other hand, the statistical treatment of sampled orbits is based on the possibility of reconstructing the probability distribution functions of the orbits by means of the histograms of their sampled versions. If the chaotic map used for encryption has good characteristics from the statistical point of view, then it is not possible to infer the value of the control parameter(s) from the obtained histograms. Conversely, a bad chaotic map generates histograms depending on the value of the control parameter(s). A way to use this dependency for cryptanalysis is by the Wootters' distance [16] between different histograms. In this sense, the histogram obtained from the sampled orbit leaked by the cryptosystem is compared to the histograms generated from a set large enough of control parameter(s). The control parameter that generates the closest histogram to the one obtained from the sampled orbit is considered as an estimation of the control parameter used for the encryption. Figure 3 illustrates the success of this estimation method for the logistic map.

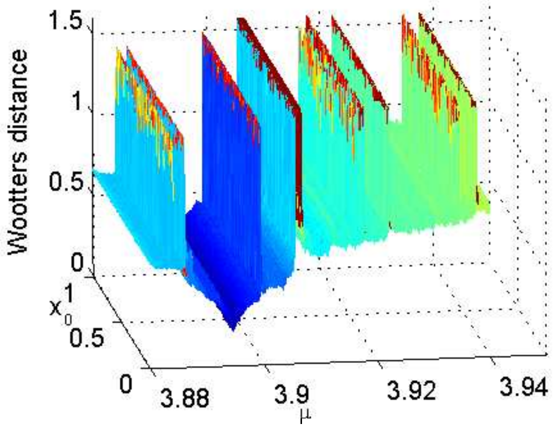


Figure 3. Estimation of the control parameter of the logistic map by means of the Wootters' distance. The value of μ and the initial condition x_0 used in the generation of the orbit were $\mu = 3.8947192$ and $x_0 = 0.99842379$.

4.2. Analysis of entropy

In the context of chaos-based cryptography the space of cryptograms has an entropy determined mostly by the underlying chaotic system. Therefore, it is very important to verify that the measure of entropy obtained through the cryptograms does not allow to guess segments of the plaintext or to get a one-to-one relationship with respect to the control parameter(s) of the underlying chaotic system. In this sense, when selecting the chaotic map and the encryption architecture, it is highly advisable to evaluate first the entropy of the orbits generated from the map. If this analysis is not done, then it could be possible for the cryptanalyst to build an attack upon different measures of entropy depending on the kind of information contained in the cryptograms. This is the case of the attack performed in [18] on Shannon's measure of entropy. Other measures of entropy that could be useful for cryptanalysis are the topological entropy [19] and the wavelet entropy [20].

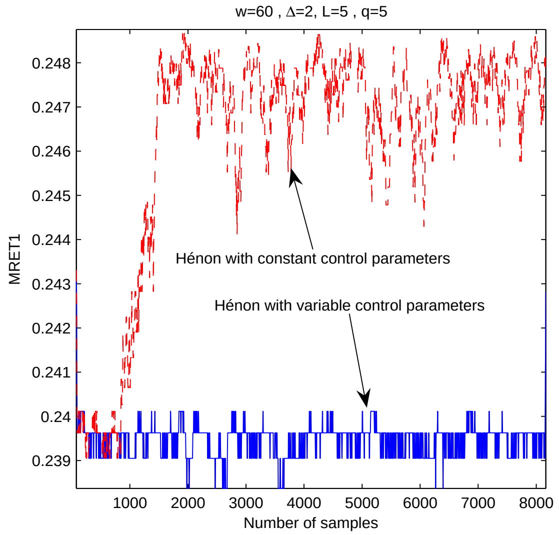


Figure 4. First level of detail of the MultiResolution Entropy of Tsallis of the Hénon map with fixed and variable control parameters. See [17] for more details about the procedure.

Related to the topological entropy, in the context of digital chaos-based cryptosystems, i.e., when dealing with chaotic maps it is advisable to work with approximations of the topological entropy based on the study of permutations [21], which allows to develop a theory of discrete chaos [22] with clear interest for cryptanalysis [23]. On the other hand, the use of wavelets for the determination of measures of entropy can be an aid in the analysis of the security of chaos-based cryptosystems. For example, the theory of wavelets and the figures of entropy defined by Shannon and Tsallis can be combined to define a MultiResolution Entropy analysis that allows to identify changes in the dynamics of a certain dynamical system [17] (see Fig. 4). The detection of this changes can lead to the recovery of information or the guessing of the key or part of the key of a chaotic cryptosystem, and it can also be performed through the study of the permutations of the output sequence of the cryptosystem [24].

4.3. Analysis of statistical complexity

Another way of getting benefit from the statistical evaluation of the output of a chaos-based cryptosystem is based on the notion of statistical complexity [25]. The statistical complexity measures the level of local divergence that exists in a dynamical system with respect to the underlying periodic behavior and, consequently, can be used as a causality indicator. In this sense, the statistical complexity has been proposed as a test for the evaluation of the quality of random number generators [26–28]. Nevertheless, this is not its only application in the context of cryptanalysis, since it can also be used to find one-to-one relationships with respect to the control parameters and, as a result, it could be a hint for control parameters estimation [29]. As an example, the statistical complexity of the logistic map with respect to μ is shown in Fig. 5 and it proves that the estimation of μ is possible through the statistical complexity for certain intervals inside the definition space of the control parameter.

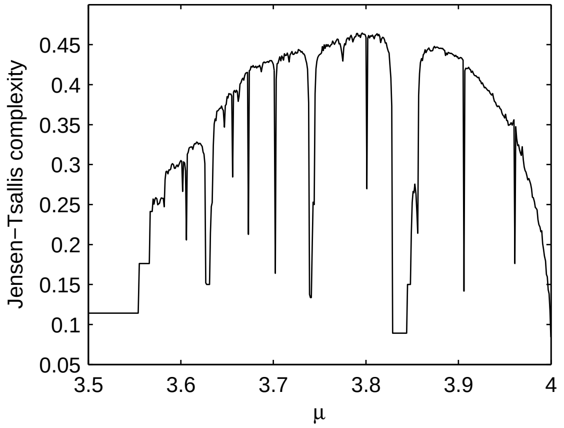


Figure 5. Jensen-Tsallis statistical complexity of the logistic map for different values of μ.

4.4. Symbolic dynamics

The study of the dynamics of unimodal maps through a discretized version of their phase space is a well known area of study in the context of the theory of dynamical systems since the seminal contribution of [30]. The conclusions derived from this work has been used for the estimation of the initial condition and the control parameter values that lead to a certain discretized version of an orbit associated to an unimodal map [31, 32], which is the base of the cryptanalysis done in [18,33,34]. However, the theory of symbolic dynamics, i.e., the study of those discretized versions of orbits of chaotic maps is not limited to unimodal maps. Indeed, the possibility of applying this kind of methodology is based on the underlying periodicity that sustained chaos. In other words, if the phase space of a chaotic map is partitioned conveniently and a symbol is assigned to each of the derived intervals, then it is possible to get the unstable periodic orbits of the system and, consequently, to reconstruct its dynamics [35–38]. This is very interesting from the point of view of cryptanalysis, since it allows to estimate the control parameter and even, in some situations, the initial condition used in the generation of a time-series from a given chaotic system [39, 40].

5. CONCLUSIONS

The present work is a summary of different methods based on the theory of dynamical systems that can be used to point out some design problems in chaos-based cryptosystems. The main conclusion derived from the set of tools proposed is that the tests of security of conventional cryptography are not the only to be considered in the context of chaotic cryptography. Indeed, either the design or the analysis of a chaotic cryptosystem must be done along with a thoroughly knowledge about the dynamics of the chaotic map selected. Otherwise, the resulting encryption scheme could present serious security and efficiency problems.

6. REFERENCES

[1] L.M. Pecora and T.L. Carroll, "Synchronization in chaotic systems," *Phys. Rev. Lett.*, vol. 64, no. 8, pp. 821–824, 1990.

[2] Claude Shannon, "Communication theory of secrecy systems," *Bell Sys. Tech. J.*, vol. 28, pp. 656–715, 1949.

[3] Robert C. Hilborn, *Chaos and nonlinear dynamics*, Oxford University Press, 2nd edition edition, 2000.

[4] Gonzalo Alvarez, F. Montoya, M. Romera, and G. Pastor, "Cryptanalysis of a discrete chaotic cryptosystem using external key," *Physics Letters A*, vol. 319, pp. 334–339, 2003.

[5] David Arroyo, Chengqing Li, Shujun Li, and Gonzalo Alvarez, "Cryptanalysis of a computer cryptography scheme based on a filter bank," p. In Press, Accepted by Chaos, Solitons and Fractals in January 2008.

[6] Gonzalo Alvarez and Shujun Li, "Some basic cryptographic requirements for chaos-based cryptosystems," *Int. J. Bifurc. Chaos*, vol. 16, no. 8, pp. 2129–2151, 2006.

[7] G. Alvarez, F. Montoya, M. Romera, and G. Pastor, "Cryptanalyzing a discrete-time chaos synchronization secure communication system," *Chaos, Solitons & Fractals*, vol. 21, no. 3, pp. 689–694, julio 2004.

[8] S. Li, G. Alvarez, G. Chen, and X. Mou, "Breaking a chaos-noise-based secure communication scheme," *Chaos*, vol. 15, no. 1, pp. 13703, marzo 2005.

[9] David Arroyo, Gonzalo Alvarez, Shujun Li, Chengqing Li, and Juana Nunez, "Cryptanalysis of a discrete-time synchronous chaotic encryption system," *Physics Letter A*, vol. 372, no. 7, pp. 1034–1039, 2008.

[10] Bingo Wing-Kuen Ling, Charlotte Yuk-Fan Ho, and Peter Kwong-Shun Tam, "Chaotic filter bank for computer cryptography," *Chaos, Solitons and Fractals*, vol. 34, pp. 817–824, 2007.

[11] E. Alvarez, A. Fernández, P. García, J. Jim'enez, and A. Marcano, "New approach to chaotic encryption," *Physics Letters A*, vol. 263, pp. 373–375, 1999.

[12] A. N. Pisarchik, N. J. Flores-Carmona, and M. Carpio-Valadez, "Encryption and decryption of images with chaotic map lattices," *Chaos*, vol. 16, no. 3, pp. art. no. 033118, 2006.

[13] A.J. Menezes, P.C van Oorschot, and S.A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 1997.

[14] Adrian Skrobek, "Approximation of a chaotic orbit as a cryptanalytical method on Baptista's cipher," *Physics Letters A*, vol. 372, no. 6, pp. 849–859, 2008.

[15] David Arroyo, Rhouma Rhouma, Gonzalo Alvarez, Shujun Li, and Veronica Fernandez, "On the security of a new image encryption scheme based on chaotic map lattices," *Chaos: An Interdisciplinary Journal of Nonlinear Science*, vol. 18, pp. 033112, 7 pages, 2008.

[16] A. P. Majtey, P. W. Lamberti, M. T. Martin, and A. Plastino, "Wootters' distance revisited: a new distinguishability criterium," *Eur. Phys. J. D*, vol. 32, pp. 413–419, 2005.

[17] L. G. Gamero, A. Plastino, and M. E. Torres, "Wavelet analysis and nonlinear dynamics in a nonextensive setting," *Physica A: Statistical and Theoretical Physics*, vol. 246, no. 3-4, pp. 487–509, 1997.

[18] Gonzalo Alvarez, Fausto Montoya, Miguel Romera, and Gerardo Pastor, "Cryptanalysis of an ergodic chaotic cipher," *Physics Letters A*, vol. 311, pp. 172–179, 2003.

[19] R. L. Adler, A. G. Konheim, and M. H. McAndrew, "Topological entropy," *Transactions of the American Mathematical Society*, vol. 114, no. 2, pp. 309–319, 1965.

[20] O.A. Rosso, S. Blanco, J. Yordanova, V. Kolev, A. Figliola, M. Schrmann, and E. Basar, "Wavelet entropy: a new tool for ananlysis of short duration brain electrical signals," *Journal of Neuroscience Methods*, vol. 105, pp. 65–75, 2001.

[21] Christoph Bandt, Gerhard Keller, and Bernd Pompe, "Entropy of interval maps via permutations," *Nonlinearity*, vol. 15, pp. 1595–1602, 2002.

[22] L. Kocarev, J. Szczepanski, J.M. Amigo, and I. Tomovski, "Discrete chaos-i: Theory," *Circuits and Systems I: Regular Papers, IEEE Transactions on*, vol. 53, no. 6, pp. 1300–1309, June 2006.

[23] J.M. Amigo, L. Kocarev, and J. Szczepanski, "Discrete Lyapunov exponent and resistance to differential cryptanalysis," *Circuits and Systems II: Express Briefs, IEEE Transactions on*, vol. 54, no. 10, pp. 882–886, Oct. 2007.

[24] Yinhe Cao, Wen-wen Tung, J. B. Gao, V. A. Protopopescu, and L. M. Hively, "Detecting dynamical changes in time series using the permutation entropy," *Phys. Rev. E*, vol. 70, no. 4, pp. 046217, Oct 2004.

[25] M.T. Martin, A. Plastino, and O.A. Rosso, "Generalized statistical complexity measures: Geometrical and analytical properties," *Physica A: Statistical Mechanics and its Applications*, vol. 369, no. 2, pp. 439–462, 2006.

[26] C.M. González, H.A. Larrondo, and O.A. Rosso, "Statistical complexity measure of pseudorandom bit generators," *Physica A: Statistical Mechanics and its Applications*, vol. 354, pp. 281–300, 2005.

[27] H.A. Larrondo, C.M. Gonzlez, M.T. Martn, A. Plastino, and O.A. Rosso, "Intensive statistical complexity measure of pseudorandom number generators," *Physica A: Statistical Mechanics and its Applications*, vol. 356, no. 1, pp. 133–138, 2005.

[28] H.A. Larrondo, M.T. Martn, C.M. Gonzlez, A. Plastino, and O.A. Rosso, "Random number generators and causality," *Physics Letters A*, vol. 352, no. 4-5, pp. 421–425, 2006.

[29] O.A. Rosso, H.A. Larrondo, M.T. Martin, A. Plastino, and M.A. Fuentes, "Distinguishing noise from chaos," *Physical review letters*, vol. 99, pp. 154102 –1,154102–4, 2007.

[30] N. Metropolis, M.L. Stein, and P.R. Stein, "On the limit sets for transformations on the unit interval," *Journal of Combinatorial Theory (A)*, vol. 15, pp. 25–44, 1973.

[31] Xiaogang Wu, Hanping Hu, and Baoliang Zhang, "Parameter estimation only from the symbolic sequences generated by chaos system," *Chaos, solitons and Fractals*, vol. 22, pp. 359–366, 2004.

[32] Gonzalo Alvarez, David Arroyo, and Juana Nunez, "Application of gray code to the cryptanalysis of chaotic cryptosystems," in *3rd International IEEE Scientific Conference on Physics and Control (PhysCon'2007, 3rd - 7th, September 2007, Potsdam, Germany)*, Potsdam, Germany, 3rd - 7th, September 2007, IEEE IPACS.

[33] David Arroyo, Gonzalo Alvarez, Shujun Li, Chengqing Li, and Veronica Fernandez, "Cryptanalysis of a new chaotic cryptosystem based on ergodicity," http://arxiv.org/abs/0806.3183, Submitted on 19 Jun 2008.

[34] Kai Wang, Wenjiang Pei, Liuhua Zou, Aiguo Song, and Zhenya He, "On the security of 3d cat map based on symmetric image encryption scheme," *Physics Letters A*, vol. 343, pp. 432–439, 2005.

[35] Matthew B. Kennel and Michael Buhl, "Estimating good discrete partitions from observed data: Symbolic false nearest neighbors," *Phys. Rev. Lett.*, vol. 91, no. 8, pp. 084102, Aug 2003.

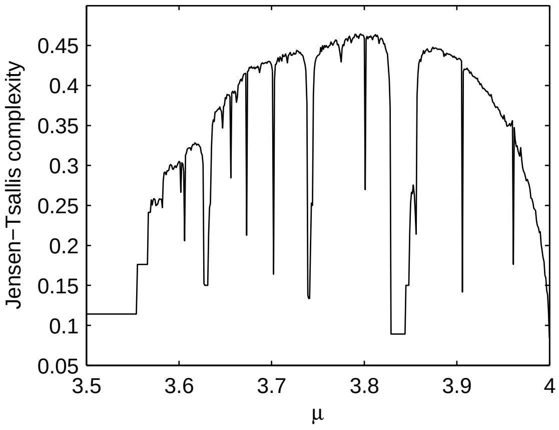
[36] Michael Buhl and Matthew B. Kennel, "Statistically relaxing to generating partitions for observed time-series data," *Physical Review E*, vol. 71, pp. 046213:1–14, 2005.

[37] Venkatesh Rajagopalan and Asok Ray, "Symbolic time series analysis via wavelet-based partitioning," *Signal Processing*, vol. 86, pp. 3309–3320, 2006.

[38] Michael Buhl and Matthew B. Kennel, "Globally enumerating unstable periodic orbits for observed data using symbolic dynamics," *Chaos: An Interdisciplinary Journal of Nonlinear Science*, vol. 17, no. 3, pp. 033102, 2007.

[39] Carlo Piccardi, "On parameter estimation of chaotic systems via symbolic time-series analysis," *Chaos*, vol. 16, pp. 043115:1–10, 2006.

[40] Kai Wang, Wengjiang Pei, Shaoping Wang, Yiu-Ming Cheung, and Zhenya He, "Symbolic vector dynamics approach to initial condition and control parameters estimation of coupled map lattices," *IEEE Transactions on Circuits and Systems-I: Regular Papers*, vol. 55, pp. 1116–1124, 2008.


Jensen−Tsallis complexity
0.45
0.4
0.35
0.3
0.25
0.2
0.15
0.1
0.05
3.5
3.6
3.7
3.8
3.9
4
μ