On the inadequacy of unimodal maps for cryptographic applications

David Arroyo * § , José María Amigó†, Shujun Li‡ and Gonzalo Alvarez*
*Instituto de Física Aplicada, Consejo Superior de Investigaciones Científicas
Email: {david.arroyo, gonzalo}@iec.csic.es
†Centro de Investigación Operativa, Universidad Miguel Hernández
Email: jm.amigo@umh.es
‡Department of Computer and Information Science, University of Konstanz
Web site: www.hooklee.com
§Present address: Instituto de Acústica, Consejo Superior de Investigaciones Científicas, Serrano 144, 28006 Madrid

This paper was published in *XI Reunión Española sobre Criptología y Seguridad de la Información* (XI RECSI), Josep Domingo Ferrer, Antoni Martínez Ballesté, Jordi Castellá Roca, and Agustí Solanas Gómez, editors, pp. 37-42, ISBN 978-84-693-3304-4, Universitat Rovira i Virgili, Tarragona, Spain, 2010.

***Abstract*—The security of chaos-based cryptosystems is closely related to the possibility of recovering control parameters and/or initial conditions from partial information on the associated chaotic orbits. In this paper we analyze this possibility for the case of unimodal maps. We show a meaningful set of contexts where the dynamics of unimodal maps can be reconstructed, which means a relevant reduction of the scope where this kind of chaotic maps can be applied to build up new encryption procedures.**

I. Introduction

Chaos-based cryptography uses chaotic systems to guide the encryption procedure inside an encryption architecture. The examination of the adequacy of a specific chaotic map for an encryption architecture is a very complex problem, and we have the feeling that a general solution to this problem cannot be found. As a matter of fact, even for non-chaos-based encryption systems, it is not possible to establish a general security evaluation procedure. Therefore, the evaluation of the security of a cryptosystem is generally an *ad hoc* procedure, and the starting point should be the set of strategies used by cryptanalysts. The first step in either the design or the security analysis of a cryptosystem is to detect the components which could be examined or studied using previous cryptanalysis techniques. In other words, it is necessary to identify the critical components of a cryptosystem before starting its design or cryptanalysis.

In the case of chaos-based cryptosystems, the identification of these critical components must focus in a first approximation on three points: the selection of the encryption architecture, the selection of the chaotic system(s) and the procedure that determines the association between the chaotic system(s) and the encryption architecture. With respect to the selection of the encryption architecture, if we assume symmetric cryptography, it is necessary to discern between stream ciphers and block ciphers. In [1, Chapters 3 and 4] a detailed analysis of various attacks on conventional stream and block ciphers can be found. For chaos-based cryptography, it is natural that those attacks should anyway be considered, by considering that now the cryptosystems under study are driven by chaos. Concerning the selection of the chaotic system(s), we have to examine thoroughly two critical aspects: (i) the complexity of the chaotic systems; (ii) the possibility of reconstructing the dynamics of the chaotic system(s) from the information leaked, in different cryptanalysis contexts associated to a given encryption architecture.

The complexity of the underlying chaotic systems depends on both their dimensionality and their physical implementation. According to Poincaré-Bendixson Theorem [2, p. 101], chaotic dynamical systems in continuous time have a phase space of dimension greater than 2. Conversely, dynamical systems in discrete time can be chaotic even when the phase space is of dimension 1, if the rule of evolution is a non-invertible function. On the other hand, chaotic systems can be implemented in analog (i.e., upon some circuitry) or in digital form. The first option is generally associated to the use of chaos synchronization techniques [3], [4], which is not the case in the second option. The digital alternative demands an analytical description of the chaotic system. If the chaotic system is described in continuous time, then its analytical definition is a set of differential equations, and the determination of its temporal evolution requires the use of numerical methods. The use of such methods informs about an extra burden (in terms of computation) when calculating the orbits of the chaotic systems. Moreover, it incorporates an extra problem, since numerical methods are defined in dependence of configuration parameters. These parameters must be selected carefully, otherwise the dynamics of the resulting orbits can be modified resulting in a non-chaotic behavior (this is the case of the cryptosystem that we have analyzed in [5]). Contrariwise, chaotic systems in discrete time are given by a set of difference equations, and their orbits can be derived straightforwardly.

With respect to the security of chaos-based cryptosystems, the synchronization techniques entail some critical problems.

The conditions required for the synchronization of different chaotic systems are too demanding and amount to weakening the security requirements of an encryption procedure. Certainly, if synchronization is used as the bearer of an encryption architecture, then the chaotic systems at both sides will work using a subset of the control parameters space. Assuming that the control parameters are the key or part of the key of a chaos-based cryptosystem, the matching sensitivity leads to a narrowing of the key space, thus lessening the computational complexity of a *brute force attack* [6]–[17]. As a result, chaotic systems in discrete time (also known as chaotic maps) are better choices when designing new encryption procedures, since they possess less computational complexity and can be used to construct cryptosystems without synchronization.

Having as aim the concretion of efficient (and secure) chaos-based cryptosystems, it seems that the best option is to select the simplest chaotic maps. This being the case, the logistic map in particular, and unimodal maps in general have been broadly used in the context of chaos-based cryptography [18]–[36]. Nevertheless, we point out that unimodal maps cannot be applied to cryptography straightforwardly. Indeed, it is necessary to examine their potentiality to build up secure cryptosystems. This analysis is performed through the evaluation of chaotic orbits as the kernel of confusion and diffusion of the encryption procedure. In this regard a quantification of the level of "chaoticity" is required, and we also need to identify those situations enabling the estimation of control parameters and/or initial conditions from observed information about the orbits.

The rest of the paper is organized towards the above-described goals as follows. First, we introduce the basic notations used in the following sections. In Sec. III the potentiality of achieving information diffusion by concealing initial conditions of unimodal maps is studied. The analysis of the potentiality for information diffusion also requires to study the dependency of the orbits on control parameters, which is discussed in Sec. IV. Furthermore, the information confusion property is studied in Sec. V by means of different measures of entropy for unimodal maps. Finally, the ergodicity of unimodal maps is analyzed in Sec. VI, which leads to the final comments and conclusions in the last section.

II. Mathematical definition of the scope under consideration

Since we are mainly interested in families of (unimodal) maps, we define an m-dimensional discrete-time dynamical system as a triple $(\Lambda,\mathcal{U},f)$, where $\Lambda\subset\mathbb{R}^d$ is the set of parameters, $\mathcal{U}\subset\mathbb{R}^m$ is the state space, and $f:\Lambda\times\mathcal{U}\to\mathcal{U}$ is the map that updates the states $x\in\mathcal{U}$ according to the rule $x\mapsto f(\lambda,x)$. Since the parameter λ is held fixed when studying the dynamical aspects, the notation $f(\lambda,x)\equiv f_\lambda(x)$ will be used. Hence, the rule that transforms an state $x_n\in\mathcal{U}$ into an state $x_{n+1}\in\mathcal{U}$ will be written as the difference equation $x_{n+1}=f_\lambda(x_n)$. Accordingly, the forward orbit generated from an initial condition $x_0\in\mathcal{U}$ is

$$\gamma^+_{f_\lambda}(x_0)=\left\{f_\lambda^{(0)}(x_0),f_\lambda^{(1)}(x_0),\ldots,f_\lambda^{(i)}(x_0),\ldots\right\},\tag{1}$$

where

$$f_\lambda^{(i)}(x_0)=\begin{cases}x_0, & \text{if } i=0\\ f_\lambda(f_\lambda^{(i-1)}(x_0)), & \text{if } i>0\end{cases}\tag{2}$$

If the map $f_\lambda(x)$ is invertible, then the dynamical system $(\Lambda,\mathcal{U},f)$ is said to be invertible; in this case, one can also defined the backward orbits in a similar way. In this paper the focus is a specific class of maps, namely, the unimodal maps, which are denoted by $\mathcal{F}$. A map $f_\lambda:\mathcal{U}\to\mathcal{U}$, where $\mathcal{U}=[a,b]\subset\mathbb{R}$, is unimodal if it is continuous, has a single turning point (usually called the critical point) x_c in $\mathcal{U}$, and is monotonically increasing (or decreasing) on the left side of x_c and decreasing (or increasing) on the right side.

Two different situations are considered in this paper:

1) The control parameter determines the maximum value of the map, being the critical point independent of the control parameter. In this case, the parametric function f_λ is given by
$$f_\lambda(x)=\lambda F(x),\tag{3}$$
where $F\in\mathcal{F}$ and $F(x_c)=F_{\max}$. The subclass of maps $f_\lambda\in\mathcal{F}$ complying with this description will be denoted by $\mathcal{F}_1$.
As representatives of the map class $\mathcal{F}_1$ we consider the following three maps: a) the logistic map, defined by the rule of evolution
$$\begin{aligned}&x_{n+1}=f_\lambda(x_n)=\lambda\cdot x_n\cdot(1-x_n)\\&\lambda\in[0,4],\ \mathcal{U}=[0,1]\end{aligned}\tag{4}$$
b) the Mandelbrot map, given by
$$\begin{aligned}&x_{n+1}=f_\lambda(x_n)=x_n^2+\lambda,\\&\lambda\in[-2,0.25],\mathcal{U}=[-2,2]\end{aligned}\tag{5}$$
and c) the (symmetric) tent map, whose difference equation is
$$x_{n+1}=f_\lambda(x_n)=\begin{cases}\lambda\cdot x_n, & \text{if } 0\le x_n<1/2,\\ \lambda\cdot(1-x_n), & \text{if } 1/2\le x_n\le 1,\end{cases}\tag{6}$$
with $\lambda\in[1,2]$, and $\mathcal{U}=[0,1]$. Strictly speaking, the Mandelbrot map is not included in the map class $\mathcal{F}$. Nevertheless, the Mandelbrot map is topological conjugate with the logistic map [37, p. 529], which implies their equivalency by means of their dynamics.
2) The critical point is given as a function of the control parameter, i.e., $x_c=f(\lambda)$. This leads to a new subclass of maps $\mathcal{F}_2$.

In this paper we consider the skew (full) tent map as a representative of the map class $\mathcal{F}_2$. This map is defined as

$$x_{n+1}=f_\lambda(x_n)=\begin{cases}x_n/\lambda, & \text{if } 0\le x_n<\lambda,\\ (1-x_n)/(1-\lambda), & \text{if } \lambda\le x_n\le 1,\end{cases}\tag{7}$$

with $\lambda\in(0,1)$, and $\mathcal{U}=[0,1]$.

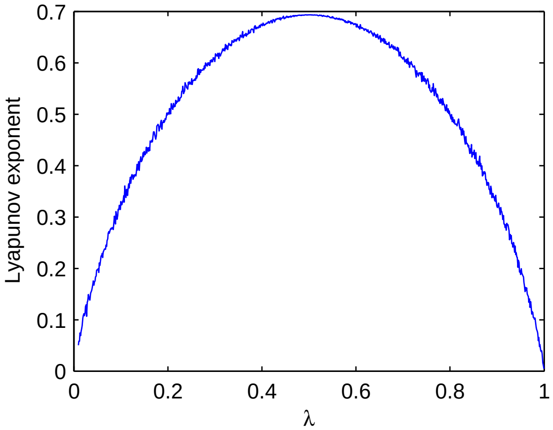


Fig. 1. Lyapunov Exponent of the skew tent map.

III. Measuring the sensitivity to initial conditions

Chaotic systems are deemed adequate for cryptography due to their high sensitivity to both initial conditions and control parameters. With respect to the initial conditions, this sensitivity can be measured by the Lyapunov Exponent (or LE in short) [38]. In this regard, if a chaotic system is used to implement an encryption scheme, then the value(s) of the control parameter(s) must be selected in such a way that the maximum LE is always positive. Quadratic maps possess a dense set of periodic windows in which the maximal LE is not positive [39]. This implies an additional complexity in the selection of adequate values for the control parameter(s). Therefore, it is advisable to use a map with a positive maximum LE for all the values of the control parameters. In this regard, the skew tent map seems to be a good option. Nevertheless, the LE of the skew tent map shows a low value for a large set of values of λ (Fig. 1), which reduces the number of valid methods of the information diffusion process built upon the orbits of the skew tent map. In other words, we should use maps exhibiting robust chaos [40], which can be generated from unimodal maps according to the scheme described in [41]. Finally, we must emphasize that the computation of the LE must be carried out taking into account finite-precision arithmetic, which is the real context of digital chaos-based cryptography. In this sense, the discrete LE [42] should be analyzed and computed.

IV. Study of the sensitivity to control parameter

One characteristic of chaotic systems is that their evolution in time is sensitive to the vector of control parameter(s) λ, i.e., two very close values of λ will eventually lead to very different orbits after a transient number of iterations. Moreover, this difference may be also present when comparing orbits as a whole, i.e, from an statistical point of view. In the context of chaos-based cryptography, it is highly advisable to avoid any kind of dependence of the statistics of the orbits on λ. If some of the statistics of the orbits can be expressed as a function of λ, then an estimation of the control parameters could be performed. For the sake of clarity, the problem is formulated mathematically as follows. Given a chaotic map $f_\lambda : \mathcal{U} \to \mathcal{U}$ and a generating partition $\mathcal{A} = A_0 \cup A_1 \cup \ldots \cup A_{N-1}$, let p_i be the probability of visiting the interval A_i is determined for $0 \leq i \leq N-1$. If the statistical behavior of the map depends on the value of λ, then $p_i = p_i(\lambda)$ and the dependency of p_i with respect to λ can be computed using some kind of statistical distance. Here, we give an example based on the *Wootters' distance* [43]. Let us consider two probability distributions $\boldsymbol{P}_i = \left\{p_j^{(i)}, j = 1, \ldots, N\right\}$ with $i = 1, 2$. The Wootters' statistical distance is given by

$$\mathcal{D}_W(\boldsymbol{P}_1, \boldsymbol{P}_2) = \cos^{-1}\left(\sum_{j=1}^{N} \sqrt{p_j^{(1)} \cdot p_j^{(2)}}\right). \tag{8}$$

If $f_\lambda : \mathcal{U} \to \mathcal{U}$ is unimodal with $\mathcal{U} = [0, 1]$, then an orbit of length M generated from $x_0 \in \mathcal{U}$ can be encoded into a binary sequence,

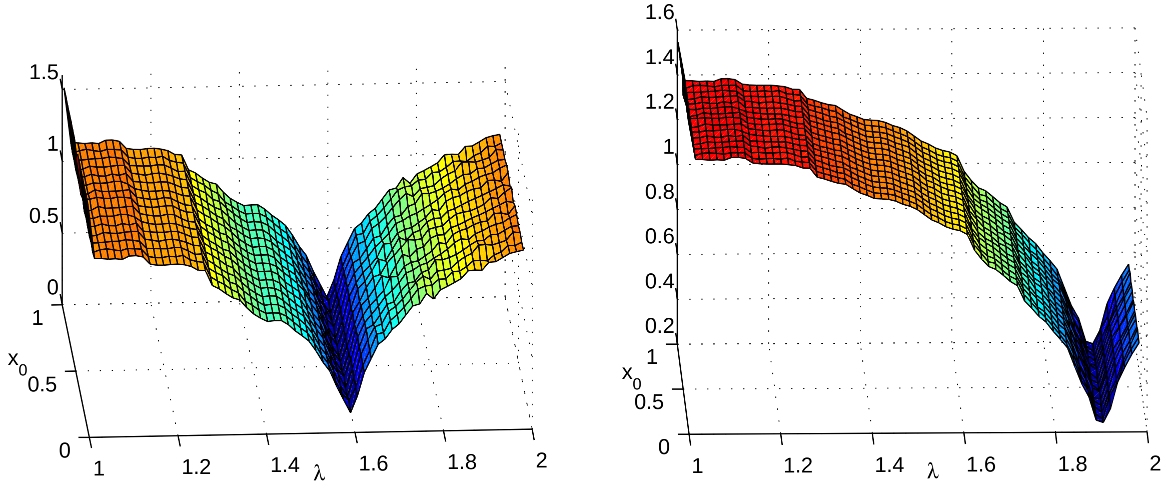
$$\begin{aligned} &\mathbf{B}_M(f_\lambda, x_0) = \{B_i(f_\lambda, x_0)\}_{i=0}^{M-1} = \\ &= \theta(f_\lambda^{(0)}(x_0))\theta(f_\lambda^{1}(x_0)) \ldots \theta(f_\lambda^{(M-1)}(x_0)), \end{aligned}$$

where $\theta(\cdot)$ is the step function

$$\theta(y) = \begin{cases} 0, & \text{if } y < x_c, \\ 1, & \text{if } y \geq x_c. \end{cases} \tag{9}$$

A probability distribution can be obtained from $\mathbf{B}_M(f_\lambda, x_0)$ by just grouping all bits in a sliding window of length w. As a result, a binary sequence of length M is transformed into a sequence of $M - w + 1$ w-bit integers (or words). The probability distribution associated to $\mathbf{B}_M(f_\lambda, x_0)$ is determined by counting the number of occurrences of each word and dividing the result by $(M - w - 1)$. Wootter's distance can be used, for example, to estimate the control parameter of the tent map. This task is carried out by computing Wootter's distance from the binary sequence $\mathbf{B}_M(f_{\hat{\lambda}}, x_0)$ (generated with an unknown value $\hat{\lambda}$ of the control parameter) to the binary sequences generated with λ ranging in an interval. These distances are computed in Fig. 2 for two values of $\hat{\lambda}$ with $M = 10^4$ and $w = 10$; the corresponding binary sequences were generated with different initial conditions. Figure 2 shows that around the right value of λ there exists a basin of attraction, which leads immediately to an estimation of $\hat{\lambda}$.

Wootters' distance can also be used to distinguish the binary sequences of a unimodal map from those corresponding to another unimodal map [44]. As a matter of fact, this is a relevant application of statistical distances in the context of unimodal maps, since the estimation of the control parameter and the initial condition can be performed from binary sequences without any auxiliary tool but the theory of symbolic dynamics [45]–[48]. In addition, we must take into account that this method is feasible only when the two maps involved are not topologically conjugate [37, p. 529].



(a)

(b)

Fig. 2. Wootters' distance of the tent map with respect to the tent map. The length of the binary sequences is $M = 10^4$, whereas the words are of width $w = 10$.

V. Analysis of chaotic orbits as source of confusion

The main appeal of chaos for cryptographic applications is based on its random-like behavior. Cryptography achieves encryption by embedding the plaintext into a source of entropy. Chaos is a source of entropy. Nevertheless, this source of entropy is conditioned by the dynamics of the specific chaotic system under consideration. Furthermore, there is not only one measure of entropies, but a large set of possible measures. In [49, Sec. 2.4] we show a set of measures of entropy, and we analyze unimodal maps by means of those measures. In that work we show that some measures of entropy show a 1-to-1 or 2-to-1 relationship with respect to the control parameter, which could represent a security flaw in the context of chaos-based cryptography.

VI. Analysis of ergodicity

In this section we point out several different critical contexts of chaos-based cryptography where the ergodic behavior of unimodal maps causes security problems.

The first critical context is given by the application of unimodal maps to the design of searching-based chaotic cryptosystems. The efficiency of searching-based chaotic cryptosystems is critically dependent on the invariant probability density function (PDF) of the orbits of the selected chaotic map. The orbits of maps, like the logistic map, the Mandelbrot map, and the tent map, possess a non-uniform PDF, which implies an important increment of the encryption/decryption time. Furthermore, the shape of the PDF of these maps depends on the control parameter(s). In some cryptosystems, as the one described in [36], the diffusion property is compromised by the dependency of the PDF on the control parameter(s). In this sense, we think that the best alternative is the skew tent map, which is a robust chaotic system, i.e., which has a uniform PDF for all the values of the control parameter. Nevertheless, schemes like the one in [36] demand not only a uniform PDF, but also a high LE.

The second critical context is the one drawn by encryption architectures where the ciphertext is obtained by sampling chaotic orbits [26], [50]. In this setting, maps such as the logistic map, the Mandelbrot map, and the tent map should not be used. Indeed, after a transient time all the values derived from the iteration of those maps are inside the interval defined by $[f_\lambda(f_\lambda(x_c)), f_\lambda(x_c)]$ [51], and the histograms of the chaotic orbits show peaks located at different images of the critical point x_c [52]. This means a leak of information about λ that can be used for its estimation, which implies a serious security flaw in the context of chaos-based cryptosystems with ciphertext obtained by sampling chaotic orbits [53], [54]. A way to avoid this critical context is to select chaotic maps with a fixed range for chaotic orbits, which is the case of the skew tent map.

The third critical context is derived from the study of ergodicity by means of order patterns. Suppose that the state space $\mathcal{U}$ is endowed with a total order $<$. Then, the elements of the orbits $\gamma^+_{f_\lambda}(x_0)$ can be arranged from the "smallest" to the "largest" according to the relation $<$. We say that $x \in \mathcal{U}$ defines the order ν-pattern $\pi = [\pi_0, \pi_1, \ldots, \pi_{\nu-1}]$ if $f_\lambda^{\pi_0}(x) < f_\lambda^{\pi_1}(x) < \ldots < f_\lambda^{\pi_{\nu-1}}(x)$. We also say that x is of type π. Observe that $[\pi_0, \pi_1, \ldots, \pi_{\nu-1}]$ is a permutation of the numbers $\{0, 1, ..., \nu - 1\}$. Order patterns can be used to detect determinism [55] and, consequently, to distinguish random systems from chaotic systems. This being the case, the isomorphism between the symbolic dynamics of a chaotic map and a random process does not mean an equivalence by means of order patterns. Actually, there always exist order ν-patterns with sufficiently large ν that are not realized in any orbit of $f \in \mathcal{F}$ [56]. In Fig. 3 the allowed order-4 patterns for the logistic map with $\lambda = 4$ are shown. For this value of the control parameter there exist twelve allowed order patterns,

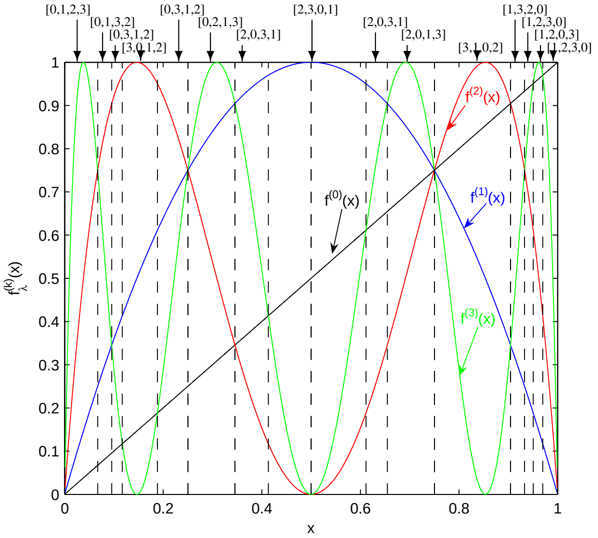


Fig. 3. $f_\lambda^{(k)}(x)$ for $k = 0, 1, 2, 3$ and the corresponding order patterns of length 4 for the logistic map when $\lambda = 4$.

which means a divergence from the twenty-four order patterns of a random system.

Another important application of order patterns is parameter estimation [57]. In general, if f_λ is a family of self-maps of the closed interval $\mathcal{U} \subset \mathbb{R}$ parameterized by $\lambda \in \Lambda \subset \mathbb{R}$ (as it occurs for $f_\lambda \in \mathcal{F}_1, \mathcal{F}_2$), and the set P_π is defined as

$$P_\pi = \{x \in \mathcal{U} : x \text{ is of type } \pi\}, \tag{10}$$

where π is an order $\nu-$pattern, then P_π depends on f_λ and, consequently, on λ. Moreover, it is assumed that f_λ is ergodic for $\Lambda \subset \mathbb{R}$ so that the orbits of f_λ can be used to build up statistics independently from the value of the initial condition. According to Birkhoff's ergodic theorem [58, p. 34], if f_λ is ergodic with respect to the invariant measure μ, then the orbit of $x \in \mathcal{U}$ visits the set P_π with relative frequency $\mu(P_\pi)$, for almost all x with respect to μ. As a result, it is possible to study the dependence of P_π on λ by counting and normalizing the occurrences of π in sliding windows of width ν along $\gamma_{f_\lambda}^{+}(x)$, x being a "typical" initial condition. Let us consider the case of the skew tent map, which possesses a known ergodic invariant measure (the Lebesgue measure) for $\lambda \in (0, 1)$ [59]. As a result, the relative frequency of the order pattern π in a typical orbit of the skew tent map, coincides with the Lebesgue measure of P_π, which can be determined analytically. For the skew tent map, the interval $P_{[0,1,\ldots,\nu-1]}$ is determined by the leftmost intersection of the iterates $f_\lambda^{\nu-2}$ and $f_\lambda^{\nu-1}$, where

$$f_\lambda^n(x) = \begin{cases} x/\lambda^n, & \text{if } 0 \le x \le \lambda^n, \\ (\lambda^{n-1} - x)/\lambda^{n-1}(1-\lambda), & \text{if } \lambda^n \le x \le \lambda^{n-1}. \end{cases} \tag{11}$$

Hence $P_{[0,1,\ldots,L-1]} = [0, \phi_L(\lambda)]$, with

$$\phi_L(\lambda) = \frac{\lambda^{L-2}}{2-\lambda}. \tag{12}$$

Since this function is 1-to-1 in the interval $0 \le \lambda \le 1$ for $L \ge 2$, with $\phi_2(0) = 1/2$, $\phi_{L\ge3}(0) = 0$, and $\phi_{L\ge2}(1) = 1$, it allows to estimate λ by estimating $\phi_L(\lambda)$ —the length of $P_{[0,1,\ldots,L-1]}$ [57].

Order patterns can be used for cryptanalysis when we have access to the whole chaotic orbit or its symbolic edition. This is the case of the scheme described in [35], where encryption is performed through a symbolic sequence of a unimodal map. As we have shown in [44], a chosen-plaintext attack on the cryptosystem defined in [35] can be used to obtain the symbolic sequence used in encryption. If the symbolic sequence was derived from the skew tent map, then the method described in [57] can be used to first determine the order patterns and second to estimate the control parameter.

VII. Conclusion

According to the different analysis shown in this paper, we conclude that unimodal maps possess a large set of vulnerabilities when considering their applications to chaos-based cryptography. However, the identification of different problems of unimodal maps is very constructive with respect to the definition of a framework to design secure and efficient chaos-based cryptosystems. This framework helps figure out how to avoid those critical contexts.

Acknowledgments

The work described in this paper was supported by *Ministerio de Ciencia e Innovación of Spain*, project CUCO (MTM2008-02194) and CODCODS (MTM2009-11820). The work of Shujun Li was supported by a fellowship from the Zukunftskolleg ("Future College") of the University of Konstanz, Germany, which is part of the "Excellence Initiative" Program of the DFG (German Research Foundation).

References

[1] M. Stamp, R. M. Low, Applied cryptanalysis: breaking ciphers in the real world, John Wiley & Sons, Inc., Hoboken, New Jersey, USA, 2007.

[2] R. C. Hilborn, Chaos and nonlinear dynamics, 2nd Edition, Oxford University Press, 2000.

[3] L. Pecora, T. Carroll, Synchronization in chaotic systems, Phys. Rev. Lett. 64 (8) (1990) 821–824.

[4] A. C. Luo, A theory for synchronization of dynamical systems, Communications in Nonlinear Science and Numerical Simulation 14 (5) (2009) 1901 – 1951.

[5] D. Arroyo, C. Li, S. Li, G. Alvarez, W. A. Halang, Cryptanalysis of an image encryption scheme based on a new total shuffling algorithm, Chaos, Solitons and Fractals 41 (5) (2009) 2613–2616.

[6] G. Alvarez, F. Montoya, M. Romera, G. Pastor, Breaking a secure communication scheme based on the phase synchronization of chaotic systems, Chaos 14 (2) (2004) 274–278.

[7] G. Alvarez, F. Montoya, M. Romera, G. Pastor, Cryptanalyzing a discrete-time chaos synchronization secure communication system, Chaos, Solitons & Fractals 21 (3) (2004) 689–694.

[8] G. Alvarez, F. Montoya, M. Romera, G. Pastor, Breaking parameter modulated chaotic secure communication system, Chaos, Solitons & Fractals 21 (4) (2004) 793–797.

[9] G. Alvarez, F. Montoya, M. Romera, G. Pastor, Breaking two secure communication systems based on chaotic masking, IEEE Transactions on Circuits & Systems II 51 (10) (2004) 505–506.

[10] G. Alvarez, S. Li, Breaking network security based on synchronized chaos, Computer Communications 27 (16) (2004) 1679–1681.

[11] G. Alvarez, S. Li, F. Montoya, M. Romera, G. Pastor, Breaking projective chaos synchronization secure communication using filtering and generalized synchronization, Chaos, Solitons & Fractals 24 (3) (2005) 775–783.

[12] S. Li, G. Alvarez, G. Chen, Breaking a chaos-based secure communication scheme designed by an improved modulation method, Chaos, Solitons & Fractals 25 (1) (2005) 109–120.

[13] G. Alvarez, L. Hernández, J. Munoz, F. Montoya, S. Li, Security analysis of communication system based on the synchronization of different order chaotic systems, Physics Letters A 345 (4) (2005) 245–250.

[14] S. Li, G. Alvarez, Z. Li, W. A. Halang, Analog chaos-based secure communications and cryptanalysis: A brief survey, in: The 3rd International IEEE Scientific Conference on Physics and Control (PhysCon 2007), September 3rd-7th 2007 at the University of Potsdam: Abstract Collection, 2007, p. 92, a complete edition available online at http://lib.physcon.ru/?item=1368 and http://www.hooklee.com/Papers/PhysCon2007.pdf.

[15] A. B. Orúe, G. Alvarez, D. Arroyo, J. Nunez, F. Montoya, Determinacin del valor de los parmetros del sistema de Lorenz y aplicacin al criptoanlisis de criptosistemas caticos, in: NoLineal 2007, 2007, p. 85.

[16] A. Orúe, V. Fernandez, G. Alvarez, G. Pastor, M. Romera, F. Montoya, Determination of the parameters for a Lorenz system and application to break the security of two-channel chaotic cryptosystems, Physics Letters A 372 (34) (2008) 5588–5592.

[17] A. Orúe, V. Fernandez, G. Alvarez, G. Pastor, M. Romera, F. Montoya, S. Li, Breaking a SC-CNN-based chaotic masking secure communication system, International Journal of Bifurcation and Chaos 19 (4) (2009) 1329–1338.

[18] M. S. Baptista, Cryptography with chaos, Phys. Lett. A 240 (1-2) (1998) 50–54.

[19] L. Kocarev, G. Jakimoski, Logistic map as a block encryption algorithm, Physics Letters A 289 (2001) 199–206.

[20] G. Jakimoski, L. Kocarev, Chaos and Cryptography: Block Encryption Ciphers Based on Chaotic Maps, IEEE Transactions on Circuits and Systems-I: Fundamental Theory and Applications 48 (2) (2001) 163–169.

[21] W. Wong, L. Lee, K. Wong, A modified chaotic cryptographic method, Comput. Phys. Comm. 138 (2001) 234–236.

[22] K. W. Wong, A fast chaotic cryptographic scheme with dynamic look-up table, Physics Letters A 298 (2002) 238–242.

[23] N. K. Pareek, V. Patidar, K. Sud, Image encryption using chaotic logistic map, Image and Vision Computing 24 (9) (2006) 926–934.

[24] J. Wei, X. Liao, K. Wong, T. Zhou, Y. Deng, Analysis and improvement for the performance of Baptista's cryptographic scheme, Physics Letters A 354 (2006) 101–109.

[25] J. Wei, X. Liao, K. Wong, T. Xiang, A new chaotic cryptosystem, Chaos, Solitons and Fractals 30 (2006) 1143–1152.

[26] A. N. Pisarchik, N. J. Flores-Carmona, M. Carpio-Valadez, Encryption and decryption of images with chaotic map lattices, Chaos 16 (3) (2006) art. no. 033118.

[27] T. Xiang, X. Liao, G. Tang, Y. Chen, K. wo Wong, A novel block cryptosystem based on iterating a chaotic map, Physics Letters A 349 (2006) 109–115.

[28] T. Gao, Q. Gu, Z. Chen, A new image encryption algorithm based on hyer-chaos, Physics Letters A 372 (4) (2008) 394–400.

[29] Y. Wang, X. Liao, T. Xiang, K.-W. Wong, D. Yang, Cryptanalysis and improvement on a block cryptosystem based on iteration a chaotic map, Physics Letters A 363 (2007) 277–281.

[30] B. W.-K. Ling, C. Y.-F. Ho, P. K.-S. Tam, Chaotic filter bank for computer cryptography, Chaos, Solitons and Fractals 34 (2007) 817–824.

[31] B. Mi, X. Liao, Y. Chen, A novel chaotic encryption scheme based on arithmetic coding 38 (5) (2008) 1523–1531.

[32] H. Yang, X. Lia, K. wo Wong, W. Zhang, P. Wei, A new cryptosystem based on chaotic map and operations algebraic, Chaos, Solitons and Fractals 40 (5) (2009) 2520–2531.

[33] T. Xiang, S. Wang, H. L, G. Hu, A novel symmetrical cryptosystem based on discretized two-dimensional chaotic map, Physics Letters A 364 (2007) 252–258.

[34] X. Wang, Q. Yu, A block encryption algorithm based on dynamic sequences of multiple chaotic systems 14 (2) (2009) 574–581.

[35] A. P. Kurian, S. Puthusserypady, Self-synchronizing chaotic stream ciphers, Signal Processing 88 (2008) 2442–2452.

[36] A. N. Pisarchik, M. Zanin, Image encryption with chaotically coupled chaotic maps, Physica D 237 (2008) 2638–2648.

[37] H.-O. Peitgen, H. Jurgens, D. Saupe, Chaos and Fractals, SpringerVerlag, 1992.

[38] C. Abraham, G. Biau, B. Cadre, On Lyapunov exponent and sensitivity, Journal of Mathematical Analysis and Applications 290 (2004) 395–404.

[39] W. Tucker, D. Wilczak, A rigorous lower bound for the stability regions of the quadratic map, Physica D: Nonlinear Phenomena 238 (18) (2009) 1923–1936.

[40] S. Banerjee, J. A. Yorke, C. Grebogi, Robust chaos, Physical Review Letters 80 (1998) 3049–3052.

[41] J. M. Aguirregabiria, Robust chaos with variable Lyapunov exponent in smooth one-dimensional maps, Chaos, Solitons and Fractals 42 (2009) 2531–2539.

[42] J. M. Amigó, L. Kocarev, J. Szczepanski, On some properties of the discrete Lyapunov exponent, Physics Letters A (2008) 6265–6268.

[43] A. P. Majtey, P. W. Lamberti, M. T. Martin, A. Plastino, Wootters' distance revisited: a new distinguishability criterium, Eur. Phys. J. D 32 (2005) 413–419.

[44] D. Arroyo, G. Alvarez, J. M. Amigó, S. Li, Cryptanalysis of a family of self-synchronizing chaotic stream ciphers, Communications in Nonlinear Science and Numerical Simulation, Accepted April 23.

[45] N. Metropolis, M. Stein, P. Stein, On the limit sets for transformations on the unit interval, Journal of Combinatorial Theory (A) 15 (1973) 25–44.

[46] G. Alvarez, F. Montoya, M. Romera, G. Pastor, Cryptanalysis of an ergodic chaotic cipher, Physics Letters A 311 (2003) 172–179.

[47] X. Wu, H. Hu, B. Zhang, Parameter estimation only from the symbolic sequences generated by chaos system, Chaos, solitons and Fractals 22 (2004) 359–366.

[48] D. Arroyo, G. Alvarez, S. Li, C. Li, V. Fernandez, Cryptanalysis of a new chaotic cryptosystem based on ergodicity, International Journal of Modern Physics B 23 (5) (2009) 651–659.

[49] D. Arroyo, Framework for the analysis and design of encryption strategies based on discrete-time chaotic dynamical systems, Ph.D. thesis, ETSIA of the Polytechnic University of Madrid, Madrid, Spain, avalaible online at http://digital.csic.es/handle/10261/15668 (July 2009).

[50] E. Alvarez, A. Fernández, P. García, J. Jiménez, A. Marcano, New approach to chaotic encryption, Physics Letters A 263 (1999) 373–375.

[51] J. Guckenheimer, Sensitive dependence to initial conditions for one dimensional maps, Communications in Mathematical Physics 70 (2) (1979) 133–160.

[52] R. V. Jensen, C. R. Myers, Images of the critical point of nonlinear maps, Physical Review A 32 (2) (1985) 1222–1224.

[53] G. Alvarez, F. Montoya, M. Romera, G. Pastor, Cryptanalysis of a chaotic encryption system, Physics Letters A 276 (2000) 191–196.

[54] D. Arroyo, R. Rhouma, G. Alvarez, S. Li, V. Fernandez, On the security of a new image encryption scheme based on chaotic map lattices, Chaos: An Interdisciplinary Journal of Nonlinear Science 18 (2008) 033112, 7 pages.

[55] J. M. Amigó, L. Kocarev, J. Szczepanski, Order patterns and chaos, Physics Letters, Section A: General, Atomic and Solid State Physics 355 (1) (2006) 27–31.

[56] J. M. Amigó, S. Elizalde, M. B. Kennel, Forbidden patterns and shift systems, Journal of Combinatorial Theory, Series A 115 (2008) 485–504.

[57] D. Arroyo, G. Alvarez, J. M. Amigó, Estimation of the control parameter from symbolic sequences: Unimodal maps with variable critical point, Chaos: An Interdisciplinary Journal of Nonlinear Science 19 (2009) 023125, 9 pages.

[58] P. Walters, An Introduction to Ergodic Theory, Vol. 79 of Graduate Texts in Mathematics, Springer-Verlag, New York, 1982.

[59] L. Billings, E. M. Bollt, Probability density functions of some skew tent maps, Chaos, solitons and fractals 12 (2) (2001) 365–376.