Universidad Politécnica de Madrid
Escuela Técnica Superior de Ingenieros Agrónomos

Dpto. de Física y Mecánica Fundamentales y Aplicadas a la Ingeniería Agroforestal
Área de conocimiento de Física Aplicada y Matemática Aplicada

TESIS DOCTORAL

Framework for the analysis and design of encryption strategies based on discrete-time chaotic dynamical systems

Autor:
David Arroyo Guardeño
Ingeniero Superior de Telecomunicación

Directores:
D. Gonzalo Álvarez Marañón
Doctor en Informática
D. Gerardo Pastor Dégano
Doctor en Ciencias Físicas

Año: **2009**

TRIBUNAL

Tribunal nombrado por el Mgfco. y Excmo. Sr. Rector de la Universidad Politécnica de Madrid, el día ..... de ..... de 2009.

PRESIDENTE:

SECRETARIO:

VOCAL:

VOCAL:

VOCAL:

SUPLENTE:

SUPLENTE:

Realizado el acto de defensa y lectura de Tesis el día ..... de ..... de 2009, en la E.T.S. de Ingenieros Agrónomos de la Universidad Politécnica de Madrid.
Calificación:

EL PRESIDENTE LOS VOCALES

EL SECRETARIO

AGRADECIMIENTOS

Esta tesis no hubiera sido posible sin la ayuda, comprensión y, sobre todo, paciencia de un conjunto de personas.

En primer lugar, quiero agradecer a Gonzalo Álvarez y Gerardo Pastor, directores de esta tesis, su interés, apoyo y confianza. A ellos debo mis primeros pasos en la investigación y el haber contado con las herramientas adecuadas para concretar este trabajo. A Fausto Montoya agradezco el haberme dado cabida en el Departamento de Tratamiento de la Información y Codificación del Instituto de Física Aplicada del Consejo Superior de Investigaciones Científicas, así como sus consejos y sabias apreciaciones en momentos de dificultad. También quiero agradecer la colaboración de todos los compañeros con los que he firmado artículos a lo largo de estos años, subrayando la impagable labor de Miguel Romera y la deuda que tengo para con los consejos y notas de sabiduría de José María Amigó y Shujun Li.

En segundo lugar me gustaría destacar el trato sumamente cordial que he recibido por parte de los miembros del Departamento de Física y Mecánica Fundamentales y Aplicadas a la Ingeniería Agroforestal de la Escuela Técnica Superior de Ingenieros Agrónomos de la Universidad Politécnica de Madrid. A mi tutora Rosa María Benito debo el haber encontrado un programa de doctorado idóneo para el tema de investigación abordado en esta tesis. Gracias a su ayuda y su valioso tiempo he podido encauzar convenientemente esa serie de elementos que constituyen la circunstancia de toda tesis. A este respecto, también quiero agradecer la disposición, consejos y amabilidad de Juan Carlos Losada.

Las dudas, la frustración, el desaliento hubieran sido obstáculos insalvables de no haber tenido tan buenos compañeros de trabajo. A todos ellos: muchas gracias.

La realización de esta tesis no hubiera sido posible sin el suficiente soporte económico. En primer término, agradezco al *Ministerio de Educación y Ciencia de España* el haberme otorgado una beca de Formación de Personal Investigador asociada al

proyecto de investigación con referencia SEG2004-02418. Asimismo, el trabajo de investigación acometido ha sido financiado por el *Ministerio de Ciencia y Tecnología de España* (Proyecto con referencia TSI2007-62657), por el *CDTI, del Ministerio de Industria, Turismo y Comercio de España* en colaboración con Telefónica I+D (Proyecto SEGUR@ con referencia CENIT 2007-2010), por el *CDTI, Ministerio de Industria, Turismo y Comercio de España* en colaboración con SAC (Proyecto HESPERIA con referencia CENIT 2006-2009), y por el *Ministerio de Ciencia e Innovación de España* (Proyecto CUCO con referencia MTM2008-02194).

El último párrafo quiero dejarlo para mi familia y para Ella. Antonio y Mari, mis padres, Paula, mi abuela, la otra Mari y Elena, mis hermanas, estamos en ello y según parece a algún sitio hemos llegado. Y a ti Cristina, lo que te quiero decir no es una frase, es una vida.

A todos, sinceramente, gracias.

RESUMEN

De acuerdo con la teoría de la información desarrollada por Claude Shannon[1], un *buen* sistema de cifrado está basado en la transformación de la información mediante operaciones de mezcla dependientes de un parámetro o conjunto de parámetros externos, el cual hará las veces de clave secreta del sistema. En una situación ideal dicho sistema presenta una gran dependencia respecto al texto cifrado y a la clave, de modo que pequeños cambios en los mismos conducen a textos cifrados totalmente distintos. El objetivo es que el texto obtenido en el proceso de cifrado sea estadísticamente independiente tanto del texto en claro (o texto a cifrar) como de la clave empleada. Según Shannon, una estrategia adecuada para lograr este objetivo sería aquella fundamentada en la concatenación de un par de operaciones simples no conmutativas. De forma más precisa, Shannon alude a la necesidad de efectuar sucesivas *compresiones* y *expansiones* del texto a cifrar, de forma análoga al comportamiento analizado por Hopf[2]. De este modo, Shannon define las características esenciales del cifrado de información aludiendo implícitamente a algunas de las propiedades que identifican a los sistemas dinámicos caóticos. En efecto, el caos se caracteriza por presentar un comportamiento con una alta divergencia local (expansión) y una convergencia global (compresión) que, en último término, determinan una alta dependencia respecto a las condiciones iniciales y el conjunto de parámetros de control. Asimismo, esa paradójica asociación entre divergencia y convergencia hace que los sistemas caóticos presenten una propiedad de mezcla de gran utilidad a la hora de diseñar estrategias de cifrado de información. En este sentido, se pueden adoptar dos posibles planteamientos. Una primera opción es diseñar mecanismos de cifrado basados en *técnicas de sincronización* de sistemas dinámicos definidos en tiempo continuo. La otra posibilidad es trabajar en tiempo discreto. La técnicas de cifrado fundamentadas en la sincronización de sistemas dinámicos se han mostrado intrínsicamente inseguras y, por ello, en esta tesis nos centramos en el análisis de criptosistemas basa-

[1] C. Shannon, "Communication theory of secrecy systems," Bell Sys. Tech. J., v. 28, pp. 656-715, 1949

[2] E. Hopf, "On Causality, Statistics and Probability," Journal of Math. and Physics, v. 13, pp. 51-102, 1934.

dos en sistemas dinámicos definidos en tiempo discreto, a los que nos referiremos en lo que sigue como *mapas*.

Un sistema dinámico caótico está matemáticamente definido por un conjunto de ecuaciones que, de forma genérica, dependen de un conjunto de parámetros externos. Estos parámetros controlan la dinámica de los sistemas dinámicos involucrados, de modo que es posible que para diversas configuraciones la dinámica generada no sea caótica. Dicho de otra forma, cuando un sistema dinámico caótico está definido de forma paramétrica no se puede asumir sin más el comportamiento caótico del sistema para todas las configuraciones posibles. Dado que el uso de tales sistemas en el contexto de la criptografía requiere su comportamiento caótico, el primer paso a llevar cabo será el de establecer mecanismos verificadores del mismo. Para ello es necesario en primer término clarificar en qué se fundamenta el uso de sistemas caóticos como soporte de nuevos criptosistemas. Tal y como se ha mencionado anteriormente, uno de los elementos que hace atractivo el caos para la criptografía es su alta sensibilidad a las condiciones iniciales. En efecto, los sistemas caóticos se caracterizan por presentar una tasa positiva de divergencia local, la cual se puede cuantificar mediante el *exponente de Lyapunov*. Ahora bien, no basta que el sistema considerado presente un exponente de Lyapunov positivo, además es preciso que el comportamiento estadístico de las órbitas resultantes sea independiente del valor del parámetro o parámetros de control. En este sentido el sistema dinámico considerado debe dar lugar a órbitas con una función de distribución de probabilidad no dependiente del parámetro o parámetros de control. Por último, un criptosistema caótico utiliza el caos fundamentalmente como fuente de entropía y, en consecuencia, es necesario establecer el nivel de incertidumbre que se puede obtener a partir de la iteración de un cierto sistema dinámico.

Hasta este punto se cuenta con suficientes criterios para constatar la capacidad de un cierto sistema dinámico como mecanismo generador de complejidad que, en último término, será utilizada para ocultar información. Ahora bien, no podemos olvidar que la teoría del caos se desarrolló con el objetivo de modelar comportamientos caóticos mediante ecuaciones matemáticas «simples». La teoría del caos marca una transición

desde lo complejo (desde un punto de vista cualitativo) hacia lo «simple» (desde un punto de vista cuantitativo). En este punto de la tesis corresponde establecer si es viable realizar de nuevo esa transición, esto es, si la observación de las órbitas que podemos obtener de un cierto criptosistema nos permite reconstruir de alguna forma las ecuaciones que definen el sistema caótico subyacente. En el caso de la criptografía caótica el conjunto de ecuaciones que definen el sistema empleado por la arquitectura de cifrado es conocido y, por tanto, nuestro trabajo tendrá por meta el recuperar total o parcialmente las condiciones iniciales y/o los parámetros de control asociados a las órbitas consideradas. Hemos de establecer si es posible transformar de alguna forma las órbitas de un sistema caótico de modo que se puedan construir aplicaciones biyectivas con respecto a las condiciones iniciales y/o los parámetros de control. Lo fundamental de esta tarea no es sólo construir tales aplicaciones biyectivas, sino también encontrar las condiciones a satisfacer para conseguir una buena estimación de los parámetros y/o condiciones iniciales. En efecto, no siempre las órbitas obtenidas a partir de un criptosistema caótico son suficientemente «largas» como para obtener una buena estimación de los parámetros, mientras que en otras ocasiones no se tiene acceso a órbitas exactas, sino a versiones *discretizadas* o *muestreadas* de las mismas. Es más, la aplicabilidad y el éxito de una cierta metodología es dependiente de las características dinámicas del sistema considerado, por lo que no es posible establecer un conjunto de procedimientos válidos en cualquier contexto y para cualquier sistema dinámico. Es por ello que en esta tesis el trabajo se ha centrado en los mapas más utilizados en criptografía, esto es, el mapa logístico y la familia de mapas unimodales topológicamente conjugados a él. En efecto, las características dinámicas del mapa logístico permiten ilustrar con gran claridad la importancia de seleccionar adecuadamente los parámetros de control, así como el peligro de que un sistema de cifrado filtre demasiada información relativa a tales características. En este sentido, las órbitas del mapa logístico han sido evaluadas desde el punto de vista estadístico y desde la óptica del espacio de frecuencias. El objetivo ha sido poner de relieve cómo afectan los cambios de valores del parámetro de control y de la condición inicial al

nivel de entropía, a la función de distribución de probabilidad y al comportamiento frecuencial del mapa logístico. En lo que respecta a la entropía, ha de llevarse a cabo un análisis exhaustivo de la misma y, por ello, no nos podemos limitar al estudio de la entropía en el sentido de Shannon, sino que también han de ser consideradas medidas no extensivas como las propuestas por Tsallis[3]. Es de especial utilidad el estudio de la entropía desde la óptica del examen en tiempo-frecuencia que lleva a cabo la transformada wavelet, el cual permite definir el concepto de *entropía wavelet*. Otra medida de entropía definida mediante la transformada wavelet es la *entropía multiresolución*. Tal y como se muestra en esta tesis, esa manera de evaluar la entropía posibilita localizar cambios en la dinámica propiciados por modificaciones en los parámetros de control, lo cual puede hacer factible una estimación de los parámetros de control y, por tanto, tiene que ser tenido en consideración al diseñar o al comprobar la seguridad de un criptosistema caótico. De la misma forma, es obligatorio un minucioso estudio de la función de distribución de probabilidad de las órbitas del mapa caótico considerado. En el caso del mapa logístico y de los mapas unimodales topológicamente conjugados a él existe una gran dependencia de dicha función con respecto al parámetro de control. Dicha correlación queda claramente evidenciada mediante el examen de las funciones de probabilidad utilizando medidas de distancia estadística. Por último, el mapa logístico, como cualquier sistema dinámico caótico, se caracteriza por presentar un conjunto denso de órbitas inestables. En el caso del mapa logístico la densidad de tales órbitas crece a media que lo hace el nivel de entropía, detalle que queda explicitado en su complejidad estadística. La complejidad estadística en el caso del mapa logístico define una función biyectiva en la región caótica del mapa, esto es, para el conjunto de valores del parámetro de control conducentes a un comportamiento caótico. Esta circunstancia no sólo permite estimar el parámetro de control a partir de la complejidad estadística de las órbitas, sino que también lo hace factible cuando se trabaja sobre versiones binarias de las órbitas del mapa logístico. En esta línea, se transformaron las órbitas del mapa logístico en secuencias de unos y ceros

[3] C. Tsallis, "Possible generalization of Boltzmann-Gibbs statistics," Journal of Statistical Physics, v. 5(1-2), pp. 479-487, 1998

sin más que comparar cada valor de órbita con el punto crítico del mapa: un valor menor que el punto crítico es sustituido por un cero, mientras que un valor igual o mayor que el punto crítico da lugar a un uno. Las secuencias binarias así obtenidas pueden ser ordenadas en relación a la condición inicial y al parámetro de control. En esta tesis se demuestra que ese orden es correlato del orden de la condición inicial y del parámetro de control en el dominio de los números reales, lo que implica que es posible recuperar tanto la condición inicial como el parámetro de control del mapa logístico a partir de estas secuencias binarias. Ahora bien, el método que permite la estimación del parámetro de control requiere que se conozca de antemano el valor del punto crítico. Esto es factible en el caso del mapa logístico, pues su punto crítico es fijo e independiente del valor del parámetro de control. Sin embargo, éste no es el caso de todos los mapas topológicamente conjugados al mapa logístico. Así, para el caso del mapa tienda con punto crítico variable el parámetro de control determina el valor del punto crítico. En consecuencia, es preciso buscar otra alternativa al método propuesto para el mapa logístico. En esta tesis se demuestra que la solución viene dada por los *patrones de orden*. Una manera distinta de interpretar la información contenida en las órbitas de un mapa caótico es descomponiéndolas en subórbitas y ordenando los valores contenidos en cada una de esas subórbitas. Las distintas ordenaciones de los valores de cada subórbita se llaman patrones de orden, los cuales constituyen la información con la que trabajaremos en lo que sigue con el objetivo de estimar el parámetro de control de los mapas unimodales, cuando no se conoce el valor de su punto crítico. En primer lugar, es necesario clarificar que los patrones de orden de los mapas unimodales considerados en esta tesis pueden ser construidos también a partir de las secuencias binarias obtenidas por comparación con el punto crítico. Es más, el verdadero interés de nuestro trabajo reside precisamente en construir tales patrones de orden partiendo de las secuencias binarias para estimar el parámetro de control. La base de la metodología a emplear viene dada por la dependencia respecto al parámetro de control de la anchura del intervalo de condiciones iniciales que dan origen a un cierto patrón de orden. La ergodicidad de los mapas caóticos permite

vincular tal anchura con la frecuencia de aparición del patrón de orden en una órbita dada, factor que posibilita la estimación del parámetro de control a partir de las órbitas, aun cuando el punto crítico no es conocido.

El enfoque utilizado en lo precedente permite definir un paradigma de referencia a la hora de diseñar y analizar un criptosistema basado en caos. Las distintas herramientas matemáticas que han sido introducidas, así como los procedimientos puestos en liza con objeto de detectar posibles aplicaciones biyectivas respecto a condiciones iniciales y/o parámetros de control, fueron empleados para detectar problemas de seguridad en criptosistemas caóticos recientemente propuestos. En esta tesis se recogen los principales resultados que hemos logrado en el criptoanálisis de criptosistemas basados en sistemas caóticos definidos en tiempo discreto. La aplicación de las herramientas y procedimientos explicitados en nuestros trabajos de criptoanálisis nos ha permitido concretar un conjunto de recomendaciones de cara a evitar la aplicabilidad de estas herramientas por parte de un criptoanalista o atacante. Dicho de otra forma, un criptosistema en el que no se pueden aplicar las herramientas y procedimientos definidos en esta tesis, es un criptosistema seguro con respecto a los principales problemas de seguridad detectados en el marco de la criptografía caótica. A modo de conclusión en esta tesis se presentan una serie de recomendaciones con objeto de evitar aquellos problemas de seguridad y, en consecuencia, conseguir diseñar un buen sistema de cifrado basado en caos.

ABSTRACT

Since 1990s chaotic dynamical systems have been widely used to design new strategies to encrypt information. Indeed, the dependency to initial conditions and control parameters, along with the ergodicity of their temporal evolution allow the establishment of chaos as the base of new cryptosystems, i.e., of new schemes of confusion and diffusion of information. However, an optimum design in the context of chaos-based cryptography demands a thorough knowledge not only of the foundations of cryptography, but also of the dynamics and inner structure of chaos. Therefore, any proposal to use chaos in the context of cryptography must respect a series of design rules, in order to avoid the reconstruction of the dynamics of the underlying chaotic system, and to determine an optimum use of the virtues of the chaotic dynamics.

Although it is possible to use chaos to design analog cryptosystems based on synchronization techniques, this Thesis is focused on the application of *chaotic maps*, i.e., chaotic dynamical systems defined in discrete time to cryptography. In this sense, a set of mathematical tools are defined to establish the adequacy of a chaotic map as the base of a cryptosystem, and the requirements that an encryption architecture must satisfy to avoid the dynamical reconstruction of the underlying chaotic map. More precisely, this Thesis provides an extension and systematization of the results derived from the cryptanalysis of chaos-based cryptosystems.

The above goal comprises three different stages:

1. Definition of a set of mathematical tools that allow the selection of the adequate configurations of a dynamical system to implement strategies of confusion and diffusion of information.

2. Study of the most popular chaotic maps in the field of chaos-based cryptography to determine whether these maps can be used to design new cryptosystems without incurring in security problems.

3. Summary and conclusions of the first two stages. The aim is to define a set of

rules or recommendations as a guide for the design of chaos-based cryptosystems.

Recalling the first stage, its main purpose is the search of procedures to infer or estimate the initial conditions and/or the control parameters from the orbits of a chaotic map. Different scenarios are considered depending on whether complete orbits are accesible or it is only possible to work with sampled or discretized versions of the orbits. In all scenarios the goal consist in building bijective functions with respect to the initial conditions and/or the control parameters. The requirements to build these bijective functions are clarified, along with the procedures to guide the estimation of the initial conditions and/or the control parameters. In order to test the set of mathematical tools and the estimation methods, the logistic map and its associated topological conjugate maps are thoroughly studied, since these maps are the most widely used in the design of new digital chaotic cryptosystems. Specially relevant is the study of the *symbolic dynamics* and *order patterns* of unimodal maps. The study of this family of chaotic maps leads to a series of very useful results to define a set of recommendations for both the evaluation of the security of chaos-based cryptosystems and the design of encryption schemes based on chaos.

Contents

Chapter 1

Introduction

1.1 Motivation of this Thesis

From the seminal contribution of Lorenz [Lorenz63] chaos has captured the attention of the scientific community. Nonlinear Dynamics and Chaos Theory have been developed to model complex behavior using quite simple mathematical models. This paradoxical and astonishing brotherhood is very appealing when trying to explain and forecast the evolution of economical systems, biological populations, physical processes... From this point of view, Chaos Theory is the way of understanding real and complex processes, it is a methodology to simplify reality for the sake of its comprehension. But Chaos Theory is not just valid as a framework to understand the complexity of real world, it is not just *the end of a road* but also the beginning of *a long route*. Indeed, the mathematical models built by Chaos Theory can be also used as source of information instead of as summary of given information. In this sense, those models that were generated to explain and predict the behavior of systems in real world, can be used as simple and mere mathematical equations to be further manipulated in the context of a given mathematical methodology. Modern communications are very concerned with the virtues of Chaos Theory as origin of new proposals, of new procedures to transform and to bear information. An specific area of modern communications very related to Chaos Theory is cryptography, as it is implicitly pointed out in Shannon's perfect secrecy theory [Shannon49]. Certainly, the main properties of chaos are very connected to the the main properties that a well designed encryption system must possess. Nevertheless, the application of Chaos Theory to the design of new encryption schemes can not be done straightforwardly. Certainly, the "simple" mathematical models derived from Chaos Theory were developed from the analysis of the complex chaotic behavior of real systems, which implies that a similar procedure could be applied to elude the complexity of

the encryption methodologies based on those mathematical models. This Thesis is concerned with analyzing thoroughly the link between chaos and cryptography, and establishing when it is possible to elude the security emanated from the use of chaos as base of encryption systems. The concretion of both goals requires to establish clear and rigorously what the main demands of cryptography are, and how they can be fulfilled using chaotic systems. A first approximation to this concern is provided along the rest of this Chapter, whereas an exhaustive and deep study of it is fulfilled along the rest of this Thesis.

1.2 Cryptography: foundation and basic concepts

Almost from the beginning of writing language, there has been a necessity of finding means to conceal valuable information [Singh00]. Cryptology is the science involved in the transformation of information in such a way that it is not accessible for other people different from the legitimate source and destination. This process requires two steps:

1. Selection of the tools and the framework which guide the concealing of the information.

2. Evaluation of the achieved encryption scheme.

These two stages are two different but complementary branches of cryptology, which are *cryptography* and *cryptoanalysis*.

Cryptography derived from Greek *krýpto* "hidden" and the verb *gráfo* "to write"', and it is referred to the conversion of ordinary information or *plaintext* into unintelligible gibberish or *ciphertext* (also known as *cryptogram*) and viceversa [Kahn96]. The transformation of the plaintext into the ciphertext is named *encryption*, whereas the inverse operation is called *decryption*. In ancient times encryption was performed by replacing a general understandable code into a code just known by a group of selected people, which comprised the legitimate sender and receiver of the information. This was the case of Egyptian hieroglyphic. Nevertheless, this kind of encryption is impractical since it requires the code used in the exchange of information to be changed for every new sender-receiver pair. For that reason, the primitive encryption schemes were replaced by others where the code was generated using a transformation procedure depending on an external parameter, the *key*. In this sense, the sender and the receiver do not need to know the code conforming the ciphertext, they only need to know the transformation procedure and the value of the key. With the industrial

revolution, the encryption/decryption had to be changed to meet the requirements of the new communications scope. Indeed, the former cryptography handled language characters and produced language characters. However, communication through radio and telegraph requires the transformation of the language words into a new code which is a series of zeroes and ones. This is the bit era and from now on cryptography handles and transforms set of bits instead of words of a language. In this scenario, the encryption and decryption procedures are mathematical algorithms dependant on a secret key. Therefore, the encryption procedure is led by the function given by

$$E_{k_e} : \mathcal{P} \rightarrow \mathcal{C}, \tag{1.1}$$

where $k_e \in \mathcal{K}_e$, $\mathcal{K}_e$ is the encryption *key space* (i.e., the set of all possible values for the secret key k_e), $\mathcal{P} = \{p_0, p_1, \ldots, p_{|\mathcal{P}|}\}$ is the plaintext space, and $\mathcal{C} = \{c_0, c_1, \ldots, c_{|\mathcal{C}|}\}$ is the ciphertext space. On the other hand, the recovery of the plaintext is determined by the following function:

$$D_{k_d} : \mathcal{C} \rightarrow \mathcal{P}, \tag{1.2}$$

where $k_d \in \mathcal{K}_d$, being $\mathcal{K}_d$ the decryption key space. If the encryption scheme is *symmetric*, then $k_d = k_e$ and the cryptographic system or *cryptosystem* is a *secret key cryptosystem*. On the other hand, if the k_d is different from k_e, then the associated cryptosystem is called *asymmetric* or *public key cryptosystem*. In this work all the considered cryptosystems are symmetric, i.e., henceforth it is assumed that $k_e = k_d = k$, and the key space is noted as $\mathcal{K}$. The security of a cryptosystem is very dependant on the cardinality $|\mathcal{K}|$ of the key space. Indeed, the decryption procedure is a bijective function if the value of the secret key is known (see Fig. 1.1). Otherwise, the recovering of the plaintext from the ciphertext requires to apply the decryption function for every possible value of the secret key, i.e., to perform a *brute force attack*. Therefore, if the brute force attack is the only way of eluding the security of a cryptosystem, then the more possible keys, the more security.

Until this point the encryption and corresponding decryption procedures have been reduced to some kind of mathematical function. The proper selection of encryption/decryption functions must be done according to Shannon's *theory of perfect secrecy* [Shannon49]. This being the case, a secure cryptosystem must assure the statistical independency of the the output with respect to either the input and the secret key. The verification of this independency is done from the perspective of the *information theory*. In this context, either the plaintext or the ciphtertext are considered as statistical variables by means of the *amount of information* contained in them. The statistical figure involved is consequently the *entropy*. In information theory, the

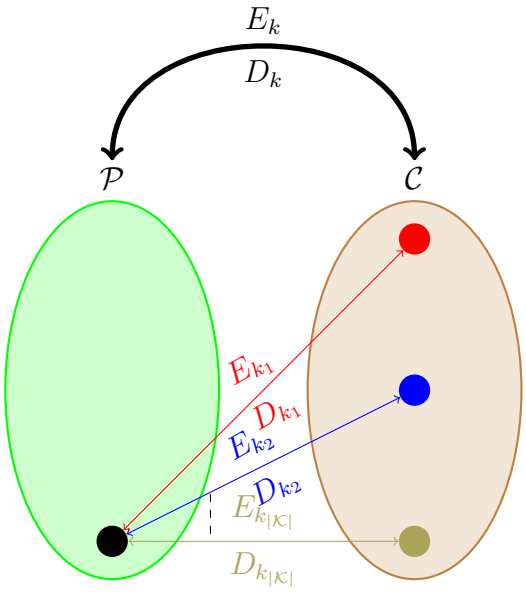


Figure 1.1: Transformation of the plaintext space $\mathcal{P}$ into the ciphertext space $\mathcal{C}$ through the encryption function $E_k(\cdot)$. Every plaintext can be associated to $|\mathcal{K}|$ images or ciphertexts. Bijective associations between plaintexts and ciphertexts are established once the key is known.

index to quantify the information emanated from any process is given by the difficulty of predicting the new events derived from the considered process. Certainly, the future behavior of any process is more difficult to anticipate if it evolves randomly. In other words, the more random is a process the more difficult is to anticipate its future evolution. The *randomness* of a process is its entropy and is defined mathematically as follows.

Definition 1.2.1 (Shannon's entropy)**.** *The Shannon entropy for a source of information defined by a discrete random variable $\mathcal{S}$ with possible values $\{s_0, s_1, \ldots, s_{M-1}\}$ is given by*

$$H(\mathcal{S}) = \sum_{i=0}^{M-1} Pr(s_i) \log_2 \left(\frac{1}{Pr(s_i)} \right), \tag{1.3}$$

where $Pr(s_i)$ is the probability that the symbol s_i is generated from the source of information $\mathcal{S}$.

The correlation or interdependency between two different sources of information can be established by means of their entropy. Let us consider two sources of information $\mathcal{R}$ and $\mathcal{S}$ with N and M symbols respectively. These two sources are independent if and only if $Pr(\mathcal{R} = R_i, \mathcal{S} = r_j) = Pr(\mathcal{R} = R_i)Pr(\mathcal{S} = s_j)$ for all $i \in \{0, \ldots, N-1\}$, and all $j \in \{0, \ldots, M-1\}$. This can be interpreted using the

entropy through the concepts of *joint entropy* and *conditional entropy*. First, the joint entropy is given the next definition.

Definition 1.2.2 (Joint entropy)**.** *The joint entropy of two sources of information* $\mathcal{R} = \{r_0, r_1, \ldots, r_{M-1}\}$ *and* $\mathcal{S} = \{s_0, s_1, \ldots, s_{N-1}\}$ *is defined as*

$$H(\mathcal{R}, \mathcal{S}) = \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} Pr(\mathcal{R} = r_i, \mathcal{S} = s_j) \log_2 \frac{1}{Pr(\mathcal{R} = r_i, \mathcal{S} = s_j)}. \tag{1.4}$$

Based on the joint entropy, the conditional entropy of a source of information with respect to other is defined as following.

Definition 1.2.3 (Conditional entropy)**.** *The conditional entropy of two sources of information* $\mathcal{R} = \{r_0, r_1, \ldots, r_{M-1}\}$ *and* $\mathcal{S} = \{s_0, s_1, \ldots, s_{N-1}\}$ *is given by*

$$H(\mathcal{R}|\mathcal{S}) = \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} Pr(\mathcal{R} = r_i, \mathcal{S} = s_j) \log_2 \frac{1}{Pr(\mathcal{R} = r_i|\mathcal{S} = s_j)}. \tag{1.5}$$

According to the definition of the joint entropy, the conditional entropy can be written as

$$H(\mathcal{R}|\mathcal{S}) = H(\mathcal{R}, \mathcal{S}) - H(\mathcal{S}). \tag{1.6}$$

Once the concept of entropy and conditional entropy have been introduced, the theory of perfect secrecy can be expressed mathematically. If the encryption function is $E_k(\cdot)$, and the decryption function $D_k(\cdot)$, then it is verified that $c_i = E_k(p_i)$ and $p_i = D_k(c_i)$. In this context, perfect secrecy implies that $H(\mathcal{C}|\mathcal{P}) = H(\mathcal{C})$ and $H(\mathcal{C}|\mathcal{K}) = H(\mathcal{P}|\mathcal{K})$ for any value of the secret key k in $\mathcal{K}$.

The only encryption system that satisfies perfect secrecy conditions is the Vernam's cipher [Vernam25] (see Fig. 1.2). In Vernam's cipher a random sequence of values is generated each time a plaintext is encrypted. This random sequence is of length equal to the length of the plaintext and is used only one time. For this reason Vernam's cipher is also called *one-time pad (OTP)*. Nevertheless, an encryption system must not only be secure but also efficient. This is not the case of Vernam's cryptosystems. As a matter of fact, the OTP cryptosystem is high-bandwith demanding as a consequence of creating and exchanging a secret key for every communication. Therefore, it is necessary to find other alternatives to encrypt information in such a way that perfect secrecy is not dramatically degraded. In the following section the different ways of overcoming this matter are introduced, considering the context of contemporary cryptography.

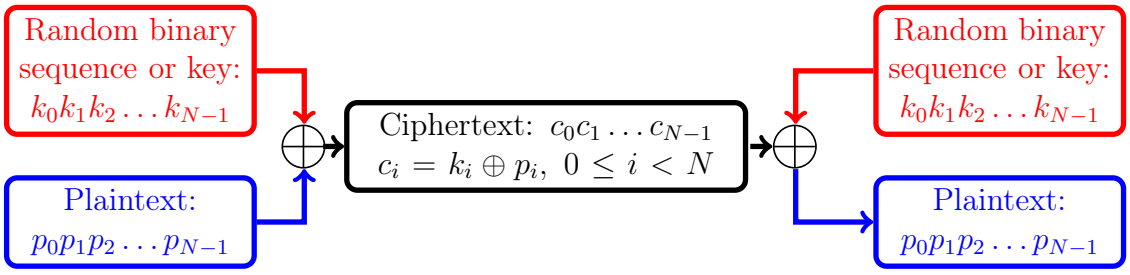


Figure 1.2: Vernam cipher.

1.2.1 Types of symmetric cryptosystems

Although Vernam's cipher provides total security, from a practical point of view its use must be discarded. Indeed, if every time a plaintext is encrypted a new key (of length equal to the length of the plaintext) has to be generated, then a key exchange must be performed before every communication, which further implies the saturation of the communication. To overcome this inner problem of Vernam's cipher, in modern cryptography two different strategies are proposed: *stream ciphers* (see Fig. 1.3) and *block ciphers* (see Fig. 1.4). As it occurs in Vernam's cipher, in

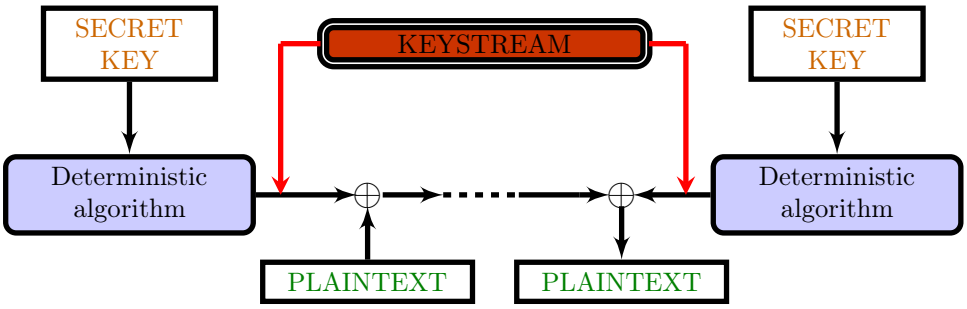


Figure 1.3: Stream cipher. The keystream is generated from the secret key according to a deterministic algorithm known by both sides of communication.

stream ciphers the transformation of the plaintext into the ciphertext is done upon every unit of information. In modern communications the unit of information is the *bit*, and thus the plaintext is a binary sequence or sequence of bits. Every bit of the plaintext is transformed into a bit of the cihpertext using a bit from a random (in the case of Vernam's cipher) or pseudorandom (in the case of stream ciphers) sequence of bits. This binary sequence is the secret key of Vernam's cipher, whereas in the context of contemporary stream ciphers is named as *keystream*. The keystream of a stream cipher is generated from the secret key using a deterministic algorithm, which avoids the key exchange before every single communication. Finally, the unit of

ciphertext is determined as the XOR between the bit of plaintext to encrypt and the corresponding bit of the keystream. The encryption strategy used in Vernam's and

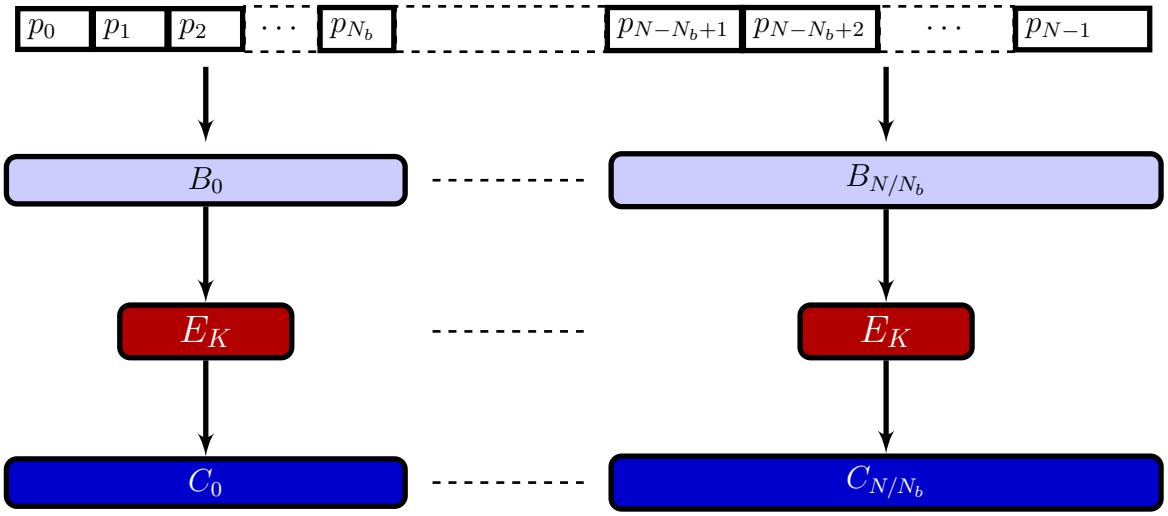


Figure 1.4: Block cipher.

stream cihpers is inherited from classical cryptography. Indeed, in both encryption schemes a unit of information is *substituted* by another unit of information according to the key or the keystream. This procedure is equivalently to classical encryption systems such as Caesar's [Kahn96, p. 73] or Vigenére's cipher [Kahn96, p. 94]. Certainly, the key of Vernam's cipher or the keystream of stream ciphers plays the same role as the pre-established displacement in Caesar's cipher or the look-up table in Vigenére's cihper. Nevertheless, substitution techniques are not the only proposals in the field of classical cryptography. Indeed, from ancient times information has been also concealed by rearranging the units of information according to the secret key. In this sense, the key of the cryptosystem leads a *transposition* of the plaintext [Kahn96, p.71]. In Shannon's work, substitution and transposition techniques are reinterpreted by means of information theory, and concludes that the security of a cryptosystem can be achieved by interleaving both techniques conveniently. This represents the fundamentals of the encryption architecture associated to *block ciphers*. However, this is not the only difference between block ciphers and stream ciphers. As a matter fact, the main divergence between these major families of encryption architectures comes from the minimum unit of information considered as input of the encryption procedure. In stream ciphers this minimum input unit of information is the bit, whereas in block ciphers is the *block*, being a block a set of bits. Therefore, in block ciphers the encryption is performed block by block and not bit by bit, as in stream

ciphers. Finally, the encryption is done combining substitution and transposition techniques, which results in an encryption procedure more complex that the one associated to stream ciphers.

Neither stream ciphers nor block ciphers meet perfect secrecy totally but just partially. Therefore, a main question arises about how to certify that the selection of encryption procedures is valid in order to avoid the access of information from non-authorized users (i.e., users that do not have the secret key). This is the main aspect covered in the following subsection.

1.2.2 Cryptanalysis: types of attacks on a cryptosystem

The perfect secrecy theory is an standard to consider, to have as a reference when designing a cryptosystem. It remarks that it is *possible* to achieve a complete protection of information, but it does not prove its *feasibility*. Indeed, modern cryptography is more concerned with the implementation of cryptosystems that assure a level of security sufficiently high to prevent any intent to subvert the protection of information. In this sense, the design of a cryptosystem must assure that the inversion of either the encryption or the decryption function can only be done if the key is known. These requirements are the core of Kerckhoffs' principle [Menezes97, p. 14] and they mean that the encryption and decryption functions are *one-way functions* [Goldreich01, p. 32]. Indeed, for a cryptosystem with a high level of security it is easy to obtain $c_i = E_k(p_i)$ but the recovery of the plaintext as $p_i = E_k^{-1}(c_i)$ is a difficult problem from the point of view of computational complexity, unless the secret key is known. If this requirement is satisfied, an attacker should perform a *brute force attack*, i.e., she should try all the values of the key to recover the plaintext from the ciphertext. The feasibility of the brute force attack depends on the size of the key space and the computational power of attackers. Furthermore, sometimes the attacker is able to use some strategies to reduce the set of keys inside the key space and used to encrypt certain plaintexts. In this situation the computational demands for an attacker are lighter and it could result in a cryptosytem's security break. The same situation is depicted with respect to the decryption function and, consequently, both the encryption and decryption functions are bijective functions if and only if the key is known. As a conclusion, the success of the intents to circumvent the security of a cryptosystem depends on the computation technology and the assessment of the security of a cryptosystem must be performed from a practical instead of theoretical point of view.

Once the plaintext has been encrypted it is sent through the public channel of information (see Fig. 1.5). The aim of cryptanalysis is to discern if it is possible

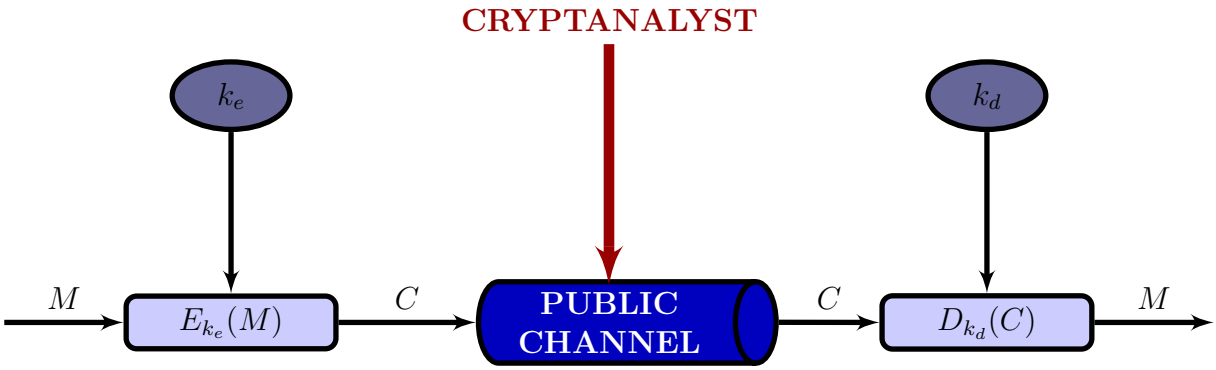


Figure 1.5: Encryption/decryption scheme.

to elude the security derived from a certain scheme. Indeed, from the cryptanalyst's point of view, the goal is either to guess the value of the secret key or to find a method to recover the plaintext from the ciphertext without knowledge of the secret key. In other words, the cryptanalyst looks for correlations between the ciphertext and the key or between the ciphertext and the plaintext. This search can be carried out from different assumptions which lead to four different cryptanalysis scenarios [Stinson95, p. 95]:

1. Ciphertext-only scenario. This is the most demanding situation from the point of view of the cryptanalyst. The attacker has only access to the ciphertext and tries to find any information from that to infer the key, part of the key, or something equivalent to the key.

2. Known-plaintext scenario. The attacker possesses one or more plaintexts and the corresponding ciphertexts. The success is based on the possibility of inferring the value of the key or the key-equivalent information from the ciphertext-plaintext pairs.

3. Chosen-plaintext scenario. In this context, the opponent has access to the encryption machinery and can choose some plaintexts and get the corresponding ciphertexts. As in the case of the known-plaintext attack, the attacker will success only if there exits a correlation between the selected pairs of plaintext-ciphertext and the key, subkey, or key-equivalent set or subset.

4. Chosen-ciphertext scenario. The attacker has access to the decryption machinery and can select ciphertexts and get the corresponding plaintexts. Again, the opponent tries to put in clear and later to exploit the correlation between

a group of selected pairs of plaintext and ciphertext and the key, subkey, or key-equivalent set or subset.

These four types of cryptographic attacks are the basic skeleton of any cryptanalysis work and, as a result, any cryptosystem must be tested in each of these scenarios in order to achieve rigorous conclusions about its security.

1.3 Chaotic cryptography

As it has been emphasized through the previous sections, the main point of cryptography is the selection of a function that transforms the plaintext space into a ciphertext space. This function must be non bijective unless additional and mandatory information is supplied. The auxiliary information that allows the inversion of the function that performs the transformation of the plaintext into the ciphertext is what it is usually called key. Therefore, cryptography deals with the searching of functions defined as

$$y = f(x, k), \tag{1.7}$$

where y is the ciphertext corresponding to the plaintext x for a given value k of the key. *Deterministic dynamical systems* are defined by a *evolution rule* that transforms the *state* of the system into a new *state*. If Eq. (1.7) is the evolution rule associated to a dynamical system, then it is possible to establish a connection between the theory of dynamical systems and cryptography. In other words, it is reasonable to question ourselves about the possibility of using dynamical systems as base of new cryptosystems. In this sense, dynamical systems should be analyzed thoroughly by means of their dynamics in order to clarify if these dynamics meet the requirements of perfect secrecy. In the following section, the concept of dynamical system is analyzed to further establish the link between the needs of cryptography and the virtues of some special type of dynamical systems.

1.3.1 Dynamical systems

A dynamical system is a model describing the temporal evolution of certain physical process from a certain initial state. The state of a dynamical system at a certain time is a vector containing m variables and is called *state vector*. The temporal evolution of the state vector determines the dynamics of the system. If there is a unique subsequent state vector to every state, then the underlying dynamical system is *deterministic*. On the other hand, if there is a probability distribution of possible subsequent state vectors, then the dynamical systems is *stochastic* or *random*. In this

work only deterministic dynamical system are considered. From a general point of view, the rule of evolution of a dynamical system not only depends on the state and time, but also on an external vector containing d variables called *control parameters*. Therefore, the rule of evolution of a deterministic dynamical system is the map

$$\varphi : \Lambda \times \mathrm{T} \times \mathcal{U} \to \mathcal{U}, \tag{1.8}$$

where $\Lambda \subset \mathbb{R}^d$ is the set of values for the control parameters, T is the set of times, and $\mathcal{U}$ is the set of all possible states of the dynamical system, i.e, the *state space* of the system. Often, the state space is called *phase space*, following a tradition from classical mechanics [Kuznetsov98, p. 2]. The set of times T can be either $\mathbb{R}$ or $\mathbb{Z}$. If $\mathrm{T} = \mathbb{R}$, then the dynamical system is a *continuous-time dynamical system* or a *flow*. On the other hand, if the set of times is $\mathbb{Z}$, then the dynamical system is a *discrete-time dynamical system* or *map* [Hirsch74, p. 140].

The considerations about the linearity of the function φ are crucial for the theory of systems dynamics. If φ is a linear function, the underlying dynamical system is called *linear*, whereas *nonlinear* dynamical systems are those associated to a function φ nonlinear. Although linear dynamical systems can be easily analyzed through an analytical procedure [Devaney89, pp. 161-172], the examination of the dynamical properties of nonlinear dynamical systems should be performed in a *qualitative* way. Indeed, the main properties of dynamical systems can be extracted by observing the temporal evolution determined by the rule of evolution φ for any $x \in \mathcal{U}$ and any $\lambda \in \Lambda$. The rule of evolution plus the set of times are linked to every set (x, λ) by a function called *orbit* or *trajectory*:

Definition 1.3.1 (Orbit or trajectory)**.** *Let us assume a dynamical system given by* $(\varphi, \mathcal{U}, \mathrm{T}, \Lambda)$*. For any* $x \in \mathcal{U}$ *and any* $\lambda \in \Lambda$*, it is defined the map* $\varphi^{(x,\lambda)} : \mathrm{T} \to \mathcal{U}$ *as* $\varphi^{(x,\lambda)}(t) = \varphi(\lambda, t, x),\ t \in \mathrm{T}$*. The image set of* $\varphi^{(x,\lambda)}$ *is* $\gamma_\varphi(x, \lambda) = \left\{\varphi^{(x,\lambda)}(t); t \in \mathrm{T}\right\} \subset \mathcal{U}$*, i.e., the* orbit *or* trajectory *associated to* x*, for a given* $\lambda \in \Lambda$*.*

Assuming we are working with *non-conservative dynamical systems*, the next point is to examine what happens in the long term with each orbit in the set of orbits associated to a dynamical system. This long term or *asymptotic behavior* leads to the concept of *invariant set*, which is the core of the qualitative theory of dynamical systems:

Definition 1.3.2 (Invariant set)**.** *Let* Γ_λ *be a subset of the phase space* $\mathcal{U}$ *of a non-conservative dynamical system given by* $(\varphi, \mathcal{U}, \mathrm{T}, \Lambda)$*. The subset* Γ_λ *is an* invariant set *of* $(\varphi, \mathcal{U}, \mathrm{T}, \Lambda)$ *if* $\Gamma_\lambda = \varphi(\Gamma_\lambda)$*. In other words, the image given by the long term temporal evolution of all the points in* Γ_λ *is the subset* Γ_λ *itself.*

There are three types of invariants:

- *Fixed point.* In this case the invariant set is given by $\Gamma_\lambda = x^*$, where $x^* \in \mathcal{U}$, $\lambda \in \Lambda$, and $\varphi^{(x^*,\lambda)}(t) = x^*$ for all $t \in \mathrm{T}$.

- *Periodic orbit.* A periodic orbit of period $t_p \in \mathrm{T}$ is an invariant set defined as $\Gamma_\lambda = \left\{\varphi^{(x,\lambda)}(t) | \varphi^{(x,\lambda)}(j \cdot t_p) = x\right\}$, where $j \in \mathbb{N}$, $x \in \mathcal{U}$, $\lambda \in \Lambda$, and $t \in T$.

- *Strange attractor.* This kind of invariant cannot be defined as the previous ones through a closed mathematical formulation and its main characteristic is the random-like behavior of all the orbits derived from it. Actually for any point inside an strange attractor the orbit that contains this point is always inside the invariant but it is neither periodic or a fixed point but *chaotic*.

Although it is generally assumed that strange attractors possess a *fractal* structure, the notion of strangeness is referred to the dynamics on the strange attractor (and not just to its geometry) [Eckmann85]. Strange attractors are the letter of presentation of *chaos*, since the properties of *chaotic systems* can be established by means of the study of the dynamics of strange attractors. According to [Devaney89, p. 50], those properties are:

1. *Sensitivity to initial conditions.* This property implies that orbits inside an strange attractor would only separate, they never meet again.

2. *Topological mixing.* Although locally nearby orbits inside an strange attractor tend to diverge one from the other, the dynamics of the set of orbits inside an strange attractor is globally confined to a finite region of the phase space. In this sense, orbits must fold back and may approach each other to diverge again in a similar way as a baker kneads dough [Peitgen92, p. 536]. This behavior also informs that the *average* long term evolution of orbits does not depend on the initial condition [Peitgen92, p. 554] and thus chaotic orbits are *ergodic*.

3. *Dense periodic points.* This is the paradox of chaos since a complex behavior, a random-like evolution in time is based on the existence of a dense distribution of periodic points, which are unstable and determine the *skeleton* of the dynamics of chaotic dynamical systems. Furthermore, strange attractors can be characterized by means of periodic orbits [Hilborn00, p.413].

4. *Sensitivity to control parameter.* This property points out that close values of λ are associated to totally different orbits.

1.3.2 Chaos and cryptography

In his milestone contribution to cryptography, Shannon points out two characteristics that any secure cipher, i.e., any well designed cryptosytem must possess [Shannon49]. Those properties are *confusion* and *diffusion*. The confusion property of a well designed cryptosytem guarantees that the ciphertext is statistically independent of the plaintext and of key. In other words, the confusion property implies the elimination from the ciphertext of any possible track or leakage of information related to either the plaintext or the key. On the other hand, the diffusion property implies that a small change in either the plaintext or the key leads to a large change in the ciphertext. As a result, two plaintexts showing a negligible difference must lead to two totally different ciphertexts and, simultaneously, very close keys transform the same plaintext into totally different ciphertexts.

The confusion and diffusion properties possess a counterpart in the domain of dynamical systems. The first and last properties of a chaotic system imply that either the initial condition or the control parameter are *diffused* through the orbits generated from a chaotic system. In other words, every single value contained in any orbit depends on the initial condition and the control parameter. This dependency is so hard that a negligible modification in either the value of the initial condition or in the value of the control parameter or both leads to an orbit completely different. As a result, chaotic systems possess a *diffusion property* of the initial condition and the control parameter with respect to the orbits. On the other hand, the mixing

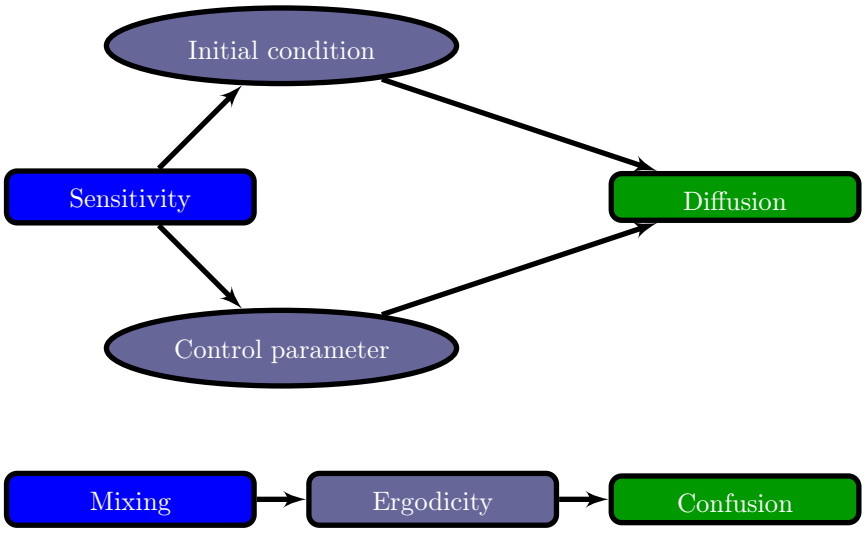


Figure 1.6: Relationship between chaos and cryptography.

property and the subsequent ergodic behavior of chaotic systems inform that the

long term evolution of chaotic orbits is independent of either the initial condition or the control parameters. At first sight it means that it is not possible to recover the exact value of either the initial condition or the control parameter or both from any statistic built upon the set of orbits generated from a chaotic system. Consequently, chaotic systems show a *confusion property* of the initial condition and the control parameters with respect to the generated orbits. Summarizing, dynamical systems can be used to implement new cryptosystems if they are chaotic, i.e., if they possess the confusion and diffusion properties with respect to the initial condition and the control parameter (see Fig. 1.6). Nevertheless, the wandering and erratic behavior of chaotic systems is sustained by an underlying periodic behavior. In other words, chaos is achieved by means of regularity, and the thorough analysis of this regularity can be used to estimate the initial condition or the control parameter. Therefore, if a chaotic system is selected for the design of a cryptosystem, it is necessary to verify that the underlying regularity of the chaotic system is concealed and not revealed by the encryption architecture. Consequently, the achievement of a good encryption scheme based on chaos requires:

1. A chaotic system with good confusion and diffusion properties.

2. An encryption architecture that makes use of the dynamics of the chaotic system to enforce the protection of the information instead of leaking the inner regularity of the chaotic system.

This Thesis is concerned with the first requirement. Digital chaos-based cryptography defines encryption procedures driven by the dynamic of one or several chaotic maps, and conditioned by a certain encryption architecture. Although some architectures are by themselves inadequate for encryption, this Thesis is focused on those whose reliability and efficiency is eroded by the dynamics of the selected map(s).

1.3.3 Selection of the chaotic system

Concerning the selection of the chaotic system, the first point is to decide between a continuous or discrete domain for the space of times T. If $\mathrm{T} = \mathbb{R}$, it is possible to build encryption schemes based on chaos using the synchronization property of chaotic systems [Pecora90]. In this case, the designed chaotic cryptosystems are called *analog chaos-based cryptosystems*. On the other hand, if $\mathrm{T} = \mathbb{Z}$ the resulting cryptosystems are called *digital chaos-based cryptosystems*. This classification entailing two types of chaos-based cryptosystems is not a mere taxonomy, since it encloses very important

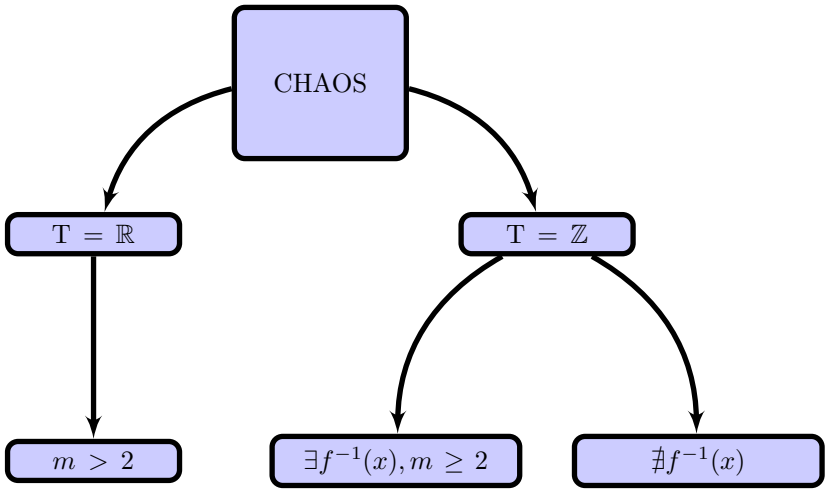


Figure 1.7: Subclass of dynamical systems possessing a chaotic attractor.

consequences for the security and efficiency of the final encryption strategies. Concerning the efficiency of a chaos-based cryptosystem, the complexity of the underlying chaotic systems must been evaluated. This complexity depends on two factors: their dimensionality and their physical implementation. First of all, the dimensionality of the chaotic system must be taken into account. According to Poincaré-Bendixson theorem [Hilborn00, p. 101], chaotic dynamical systems in continuous time have a phase space of dimension greater than 2 (see Fig. 1.7). On the other hand, dynamical systems in discrete time can be chaotic even when the phase space is of dimension $m = 1$, 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 digital form. The first option is generally associated to the use of synchronization techniques, what is not the case of the second option. The digital alternative demands an analytical description of the chaotic system. If the chaotic system is described in continuos 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 charge (by means of computation) in the derivation of 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 [Arroyo09h]). Conversely, chaotic systems in discrete time are given by a set of difference equations, and their orbits can be derived straightforwardly.

Regarding the security of chaos based cryptography, the synchronization tech-

nique entails some critical problems. The conditions required for the synchronization of different chaotic systems are too demanding and determine a divergence between them and the security requirements of an encryption scheme. Certainly, if synchronization is used as the bearer of an encryption procedure, then the chaotic systems at both sides of the communication channel are supposed to be identical. In practice, the perfect matching is not possible which forces to use not all the range of values of the control parameters, but only a subset of them. Assuming that the control parameters are the key or part of the key of a chaos-based cryptosystem, that matching sensitivity leads to a narrowing of the key space and a lessen of the computational complexity of a *brute force attack*, i.e., an attack where the cryptanalyst tries all the possible values of the secret key (see [Alvarez04b; Alvarez04e; Alvarez04c; Alvarez04d; Alvarez04a; Alvarez05b; Li05a; Alvarez05a; Li07b; Orúe07; Orúe08a; Orúe08b]). As a result, chaotic systems in discrete time are better choice when designing new encryption procedures, since they possess less computational complexity and do not need synchronization.

1.3.4 Chaotic systems considered in this Thesis

In the previous section it has been emphasized the convenience of considering chaotic systems in discrete time as base of new cryptosystems. Nevertheless, this is not the end of the road. Indeed, the family of chaotic systems in discrete time is very broad and some criterion must be established to select the best chaotic maps. In this sense, the criterion adopted in this Thesis is the *Ockham razor's principle*: the simplest, the best. First of all, the simplicity of a chaotic map is a first step to increase the efficiency of the cryptosystem. Indeed, if the iteration of the chaotic map does not involve complex mathematical operations, then the orbit can be calculated in short time. Taking into account that the orbits of the chaotic map are connected to the generation of the ciphertext, the less time to calculate the orbits, the faster the ciphertext is determined. But this is not the only one advantage of choosing simplicity as criterion for the selection of the chaotic map. As a matter of fact, a simple chaotic map can be easily understood and their dynamics can be modeled more accurately. In other words, spurious behavior is more avoidable when working on simple and well understood chaotic maps, and thus it is also easier to reduce the possibilities of successful attacks.

A simple map that has been broadly used in the context of chaos-based cryptography is the *logistic map* [May76]. The logistic map is defined as

$$x \mapsto f_\lambda(x) = f(\lambda, x) = \lambda x(1-x), \tag{1.9}$$

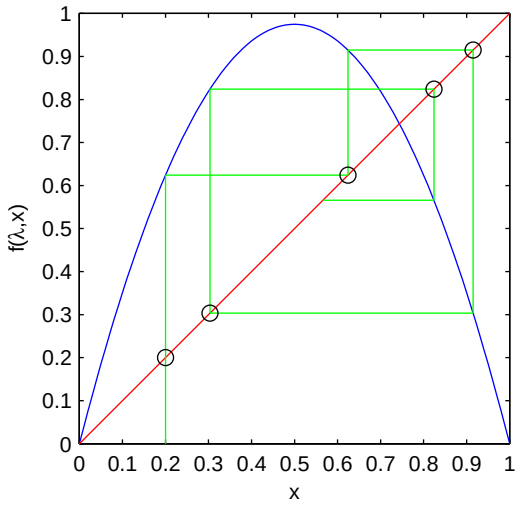


Figure 1.8: Iteration function associated to the logistic map.

where $\varphi : \mathcal{U} \times \Lambda \rightarrow \mathcal{U}$, $\mathcal{U} = [0,1] \subset \mathbb{R}$, $\lambda \in \Lambda = [0,4]$ and $x \in \mathcal{U}$. The previous equation can be used to derive an orbit from an *initial condition* $x_0 \in \mathcal{U}$ as the set of values $\{x_0, f_\lambda(x_0), f_\lambda(f_\lambda(x_0)), f_\lambda(f_\lambda(f_\lambda(x_0))), \ldots\}$. Figure 1.8 illustrates the iteration process to generate the orbit of the logistic map when the initial condition x_0 is equal to 0.2 and $\lambda = 3.9$. Actually, the logistic map is the map most widely used in the design of new digital chaotic cryptosystems [Baptista98; Kocarev01b; Jakimoski01b; Wong01; Wong02; Wong03; Tang03; Pareek03; Huang05; Pareek05; Pareek06a; Wei06a; Wei06b; Pisarchik06; Xiang06; Gao08a; Gao08b; Wang07; Ling07; Mi07; Yang08; Xiang07; Wang08b]. Some of these proposals have been totally or partially cryptanalyzed as a consequence of not fully considering the dynamical characteristics of the logistic map [Jakimoski01a; Alvarez03b; Alvarez03a; Alvarez04f; Alvarez04g; Li04b; Li07a; Arroyo09g; Alvarez07b; Skrobek08]. These cryptanalytical works are the reason of selecting the logistic map as main reference in this Thesis. Indeed, the analysis of the dynamical properties of the logistic map and their relationship with the problems pinpointed in the above cryptanalysis is very useful for the design of a general framework of cryptanalyisis work. Nevertheless, a better illustration and clarification of the concepts proposed in this Thesis can be achieved using more than one simple chaotic map. In this sense, it is considered not just the logistic map but the class of *unimodal maps*, hereafter denoted as $\mathcal{F}$.

Definition 1.3.3 (Class of maps $\mathcal{F}$)**.** *A map $\phi : \mathcal{U} \rightarrow \mathcal{U}$, where $\mathcal{U} = [a,b] \subset \mathbb{R}$, $a < b$, is unimodal if it is continuous, has a single turning point (usually called the critical point) x_c in $\mathcal{U}$, and is monotone increasing on the left of x_c and decreasing on the right. The class $\mathcal{F}$ includes maps defined in a parametric way, say, $f_\lambda(x) = f(\lambda, x)$,*

where $x \in \mathcal{U} = [a, b]$, $\lambda \in \Lambda \subset \mathbb{R}$ *is called the* control parameter*, and* f *is a map on* $\mathcal{U} \times \Lambda$.

Two different situations are considered in this Thesis:

1. The control parameter determines the maximum value of the map. In this case, the parametric function f_λ is given by

$$f_\lambda(x) = \lambda F(x), \tag{1.10}$$

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 $\mathcal{F}_1$.

2. The control parameter is the value of the critical point, i.e., $x_c = \lambda$. This leads to a new subclass of maps $\mathcal{F}_2$.

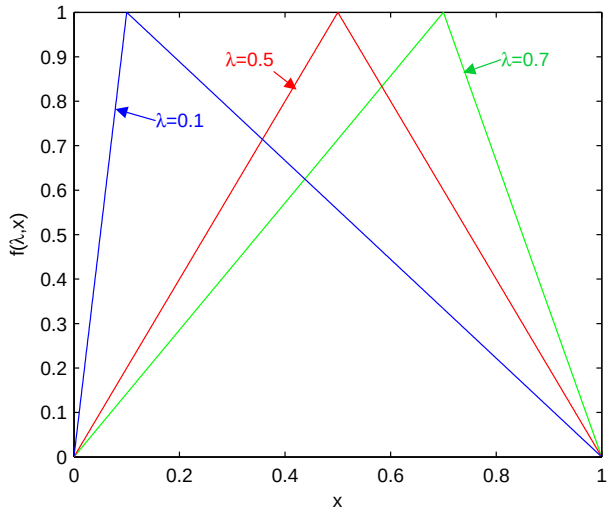


Figure 1.9: Skew tent map for different values of λ.

Among all the maps in $\mathcal{F}$, another important and relevant map is the *skew tent map*. The skew tent map is defined as

$$f_\lambda(x) = \begin{cases} x/\lambda, & \text{if } 0 \leq x < \lambda \\ (1-x)/(1-\lambda), & \text{if } \lambda \leq x \leq 1 \end{cases} \tag{1.11}$$

for $x \in [0, 1]$ and $\lambda \in \Lambda = (0, 1)$ (see Fig. 1.9). The logistic map is the representative of $\mathcal{F}_1$, whereas the skew tent map represents $\mathcal{F}_2$. In Chapter 3 the consequences of the minimal differences between $\mathcal{F}_1$ and $\mathcal{F}_2$ are shown. More precisely, it will be shown

how the results of some cryptanalysis on cryptosystems based on the logistic map can not be applied straightforward to those based on the skew tent map.

Summing up, the study of the connection between the dynamic of the maps in $\mathcal{F}$ and the problems detected in the cryptosystems built upon them, is used to achieve very useful conclusions for cryptanalysis and design of new chaos-based cryptosystems. In this Thesis the interest is on establishing a set of mathematical tools that allow the identification of the properties sustaining the link between problems of chaos-based cryptosystems and dynamics of chaotic maps. In this sense, the class of maps $\mathcal{F}$ is used to define, clarify and illustrate the use of this set of mathematical tools.

1.4 Organization of this Thesis

Once the requirements of cryptography has been made explicit, and the capacity of chaos to satisfy them has been settled, the next stage is to develop a methodology to assess if the inclusion of a given chaotic system(s) in a given encryption architecture really determines a secure encryption procedure. This analysis is performed in Chapter 2 using the class of maps in $\mathcal{F}$ as reference. Chapter 2, first of all, is concerned with the establishment of a set of mathematical tools to conclude if the properties of chaos required by cryptography are really satisfied by the selected chaotic system(s). Secondly, it is also focused on confirming if the treatment of an encryption system by means of Chaos Theory can lead to some methodology to elude the level of security that a cryptosystem should guarantee. In this sense, the theory of *Symbolic Dynamics* is specially useful. Symbolic Dynamics is an area in the Theory of Dynamical Systems that is focused on the study of discretized versions of the orbits of chaotic systems. In Chapter 3 the Theory of Symbolic Dynamics is explained for the chaotic maps in $\mathcal{F}$, pointing out that the estimation of the control parameter and the initial condition can be performed from the discretized versions of the orbits of those maps. However, it will be shown in Chapter 3 that this estimation can be accomplished only if the critical point of the map does not depend on the control parameter. In Chapter 4 it is shown how to overcome this limitation by studying the *order patterns* of the maps in $\mathcal{F}$. Either the estimation methods proposed in Chapters 3 and 4 or the mathematical tools have to be considered when designing a chaos-based cryptosystem, otherwise the final cryptosystem could present security flaws. In Chapter 5 the main problems of a negligent design are shown, and some recommendations to overcome those problems are proposed based on the theoretical framework developed in the previous Chapters. This theoretical framework, indeed,

can be used to guide the design and cryptanalysis of chaos-based cryptosystems, but it is not a closed framework. The main contributions of this Thesis are summarized in Chapter 6, which also discusses the focus of future work.

Chapter 2

Study of chaotic maps as base of digital chaos-based cryptosystems

2.1 Introduction

Chaos-based cryptography uses chaotic systems to lead the encryption procedure inside an encryption architecture. The examination of the adequacy of a chaotic map for an encryption architecture is a very complex problem, and a closed and explicit procedure cannot be provided. Certainly, even for non chaos-based encryption systems, it is not possible to establish a general security evaluation procedure. In other words, the evaluation of the security of a cryptosystem is generally an *ad hoc* procedure, and the start point must always be the set of strategies used by other cryptanalysts in other cryptanalysis. It is very important to take into account that cryptanalysis generally is focused on some aspects of a cryptosystem or set of cryptosystems. In this sense, if one can identify the properties or aspects involved in a cryptanalysis of a cryptosystem, then one is able to generalize the application of the considered cryptanalysis to other cryptosystems. Therefore, the first step in either the design or the cryptanalysis 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 controversial components of a cryptosystem before starting its cryptanalysis or design. In the case of chaos-based cryptosystems, the identification of critical components must be focused, in a first approximation in 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 [Stamp07, Chapters 3 and 4] it can be found a detailed

analysis of the main attacks on conventional stream and block ciphers. Those attacks must be considered in the context of chaos-based cryptography, but it is also necessary to remind that the encryption procedure is driven by chaotic systems. In this sense, the cryptanalysis of chaos-based cryptosystems uses the techniques inherited from conventional cryptography [Stamp07], but also the tools derived from the theory of dynamical systems. These tools lead the analysis of the orbits derived from a dynamical system and, consequently, the first thing to do is to clarify and concrete mathematically the context under evaluation in this Thesis. In this sense, a mathematical description of the orbits derived from discrete-time dynamical systems is provided in coherence with the terminology used in Chapter 1, Sec. 1.3.1. Accordingly, a discrete-time dynamical system is defined by the map $\varphi : \Lambda \times \mathbb{Z} \times \mathcal{U} \to \mathcal{U}$, where $\mathcal{U} \subset \mathbb{R}^m$, $\Lambda \subset \mathbb{R}^d$. For every $t \in \mathbb{Z}$, it is defined a map $\varphi^t : \Lambda \times \mathcal{U} \to \mathcal{U}$ given by $\varphi^t = \varphi(\lambda, x)$, with $x \in \mathcal{U}$, and $\lambda \in \Lambda$. Let us define the map $f = \varphi^1 : \Lambda \times \mathcal{U} \to \mathcal{U}$ and $f_\lambda(x) = f(\lambda, x)$ for $x \in \mathcal{U}$, and $\lambda \in \Lambda$. Upon the previous definitions, the rule that transforms an state $x_n \in \mathcal{U}$ into an state $x_{n+1} \in \mathcal{U}$ is given by a *difference equation* as

$$x_{n+1} = f(\lambda, x_n) = f_\lambda(x_n), \tag{2.1}$$

for $\lambda \in \Lambda$. Therefore, the forward orbit generated from an initial condition $x_0 \in \mathcal{U}$ is

$$\gamma^+_{f_\lambda}(x_0) = \left\{ f^{(0)}_\lambda(x_0), f^{(1)}_\lambda(x_0), \ldots, f^{(i)}_\lambda(x_0), \ldots \right\}, \tag{2.2}$$

where

$$f^{(i)}_\lambda(x_0) = \begin{cases} x_0, & \text{if } i = 0 \\ f_\lambda(f^{(i-1)}_\lambda(x_0)), & \text{if } i > 0 \end{cases} \tag{2.3}$$

A finite part of length M of the total trajectory of x_0 is given by

$$\gamma^M_{f_\lambda}(x_0) = \{x_0, x_1, \ldots, x_{M-1}\}. \tag{2.4}$$

The use of a dynamical system as base of new encryption procedure is based on the assumption that it possesses a chaotic behavior. As it is shown in Fig. 1.6, chaos can be used as the *skeleton* sustaining the confusion and diffusion properties required by any encryption system. Therefore, before using a dynamical system for cryptographical applications, it is mandatory to verify that it really has a chaotic behavior. In the context of digital chaos-based cryptography, it means that the orbits derived from the iteration of the selected map must be evaluated in order to confirm the properties that characterize and define chaos. This evaluation is performed on the long-term behavior of chaotic maps. As it is pointed out in [Eckmann85], the physical long-term behavior is on attractors and, consequently, in the rest of this Thesis it is assumed that the considered chaotic maps are non-conservative dynamical systems.

In this Chapter a collection of mathematical tools useful for that assessment is defined. First, in Sec. 2.2 it is shown how to compute the dependency on the initial conditions of the orbits of a dynamical system. This local divergence is characteristic of chaos, but it paradoxically determines a global convergence that makes up the mixing property of chaos. In Sec. 2.3 the topological mixing of chaos is studied and some mathematical figures are introduced for assessment. The analysis performed in Sections 2.2 and 2.3 is specially important for dynamical systems defined in a parametric way. Indeed, for these dynamical systems it is necessary to examine the values of the parameter controls that guarantee local divergence and ergodicity. Furthermore, it is also necessary to study how the orbits of chaotic maps can be manipulated in order to build up a secure cryptosystem. This being the case, we have to quantify the amount of information contained in a orbit, i.e., the *entropy* of orbits must be analyzed. Section 2.4 presents different methods to quantify the amount of information, but also to establish the kind of dependency of that amount of information with respect to the control parameters. This is a constant in all the work enclosed in this Chapter. The different measures here defined allow to achieve conclusions about the behavior and the adequacy of chaotic maps for chaos. Nevertheless, they are also highlights to reconstruct the dynamics of chaotic maps sustaining encryption, which could further imply the feasibility of eluding chaos-based encryption. In Sec. 2.5 another of those highlights is introduced by analyzing chaotic maps in the frequency domain using the *Wavelet Transform*. The Wavelet Transform is a very useful tool to define new measures of entropy and to detect changes in the dynamics of a chaotic map as a result of changes in the control parameters. Certainly, the dynamics of a chaotic map shows a high sensitivity to control parameters, which is very useful for cryptography since, apparently, it makes difficult to infer the value of the control parameters from the ciphertext. Nevertheless, if the ciphertext leaks too much information about the dynamics of the underlying chaotic map, it could be possible to estimate the value of the control parameters. In Sec. 2.6 this possibility is analysed by means of the statistical distance between probability distributions generated from chaotic maps. As a matter of fact, the analysis of orbits from an statistical point of view also allows to quantify the effect of the underlying order of any chaotic system, as it is pointed out in Sec. 2.7. This section analysed possible problems derived from the dense set of periodic points sustaining any chaotic behavior. Those problems are just pointed out in this Chapter, being a thorough analysis of them the main focus of the following chapters. Finally, Sec. 2.8 comments the degradation of chaotic dynamics in finite precision machines.

2.2 Measuring the sensitivity to initial conditions

As it was explained in Sec. 1.3.1, the definition of chaos implies a behavior with a high level of dependency with respect to the initial state of the system. This means that the orbits generated from very close initial conditions will separate as the time evolves, i.e., there exists a local divergence of orbits. Therefore, the sensitivity with respect to the initial state can be measured by means of the rate of divergence of orbits. The *Lyapunov Exponent* or *LE* is the figure that informs about this rate of divergence. When discrete chaotic systems or chaotic maps are considered, the LE is defined as follows [Guckenheimer83].

Definition 2.2.1. *(Lyapunov exponent) Let $(f, \mathcal{U}, \mathbb{Z}, \Lambda)$ be a dyamical system defined in discrete time with state space $\mathcal{U}$ being an open subset of $\mathbb{R}^m$, $\Lambda \subset \mathbb{R}^d$ and $f_\lambda(x) = f(\lambda, x), \forall \lambda \in \Lambda$, and $x \in \mathbb{R}^m$. Suppose that there are subspaces $V_i^{(1)} \supset V_i^{(2)} \cdots \supset V_i^{(m)}$ in the tangent space at $f^{(i)}(x)$ and numbers $LE_1(\lambda) \geq LE_2(\lambda) \geq \cdots LE_m(\lambda)$ with the properties that*

1. $Df_\lambda(V_i^{(j)}) = V_{i+1}^{(j)}$.
2. *The dimension of $V_i^{(j)}$ is $m + 1 - j$.*
3. $LE_j(\lambda) = \lim_{N \to \infty} \ln ||\sqrt{(Df_\lambda^{(N)})^T \cdot (Df_\lambda^{(N)})} \cdot v||$ *for all* $v \in V_0^{(j)} - V_0^{(j+1)}$,

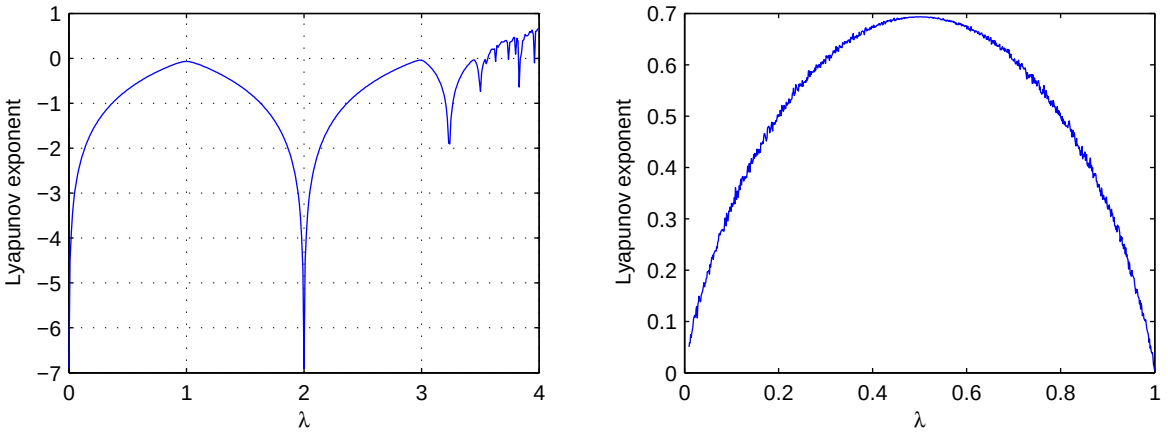
where $(Df_\lambda^{(N)})^T$ is the transpose of $Df_\lambda^{(N)}$. The Lyapunov exponent or LE is defined as the function $LE : \Lambda \to \mathcal{U}$, and is given by

$$LE(\lambda) = [LE_1(\lambda)\ LE_2(\lambda) \cdots LE_m(\lambda)]^T. \tag{2.5}$$

The LE informs about the rate of divergence of f_λ with respect to the vector of control parameters. $LE(\lambda)$ is a vector of m components. If $f_\lambda(x)$ evolves in a chaotic way, then the largest component of $LE(\lambda)$ is positive. The reciprocal implication is also valid, i.e., a positive maximal LE implies the existence of chaos.

According to the previous definition, the criterion to establish the chaoticity of a dynamical system is based on the maximal Lyapunov exponent and, consequently, it is not required to obtain the whole vector of Lyapunov exponents. However, the determination of the LE using Eq. (2.5) requires the knowledge of the analytical description of the dynamical system, whereas in the general case only orbits from the dynamical system are accesible. Therefore, it is necessary to establish some practical procedure to calculate the maximal LE. Among all the different proposals, the most efficient and accurate are those based on the computation of distances between

orbits and their further manipulation through Gram-Schmidt orthogonalization. In [Kantz94] it is explained how to compute the maximal LE upon the previous ideas. In this Thesis the maximal LE is computed according to that methodology and using the implementation included in the TISEAN package [Hegger99].



(a) (b)

Figure 2.1: Lyapunov exponent of (a) the logistic map (b) and the skew tent map.

From the perspective of chaos-based cryptography, the *LE* is a very useful tool for either the cryptologist or the cryptanalyst. In the first case, the design of any encryption scheme requires to establish explicitly and thoroughly what the secret key of the cryptosystem is and what its definition space is. In other words, the *key space* has to be totally explained. In chaos-based cryptosystems if the control parameters are part of the secret key, the values of the control parameters inside the key space are those implying the chaotic behavior of the underlying dynamical system. The identification of those values is performed with the assistance of the LE, which is done for the logistic map and for the skew tent map in Fig. 2.1. A first evaluation of the just mentioned figure emphasizes an important difference between the logistic map and the skew tent map. Indeed, the skew tent map possesses a positive LE for all the values of λ, whereas in the case of the logistic map the intervals of λ implying chaos are disjoint. A first consequence of this fact is that a cryptosystem based on the skew tent map allows a better and easier selection of keys upon the values of the control parameter. Moreover, loss of chaoticity is excluded in the case of the skew tent map, whereas in the case of the logistic map it is a critical problem that must be faced and handled by the cryptosystem's designer. However, a well designed cryptosystem is characterized by the fact that two very similar plaintexts lead to very different ciphertexts. Moreover, if the same plaintext is encrypted using two very close keys,

then the encryption procedure results in two totally different ciphertexts. For that reason, it is very convenient for the design of a chaos-based cryptosystem to use a chaotic map with a large enough Lyapunov exponent. The skew tent map fails in this requirement (see Fig. 2.1(b)). Nevertheless, it is possible to overcome this problem through the discretization of the phase space based on the following function upon $f_\lambda(x)$:

$$\hat{f}_\lambda(x) = \lfloor 2^\alpha \cdot f_\lambda(x) \rfloor \mod \Theta, \tag{2.6}$$

where $\alpha \in \mathbb{N}$ and $\Theta \in \mathbb{N}$. In Fig. 2.2 it is shown that the Lyapunov exponent of the generated sequences using Eq. (1.11) and Eq. (2.6) for $\alpha = 33, 43, 50$, is greater than the one associated to the original skew tent map for all the values of λ. In [Arroyo08c; Rhouma09] we have used the discretized version of the skew tent map to design a chaos-based cryptosystem implementing a good diffusion procedure.

Another map that shares with the logistic map the *LE's flaw* is the *Hénon map* [Hénon76]. The state space of the Hénon map is defined in $\mathbb{R}^2$ and possesses two control parameters $\delta, \beta \in \mathbb{R}$. The analytical definition of the Hénon map is:

$$x_{k+1} = \begin{bmatrix} u_{k+1} \\ v_{k+1} \end{bmatrix} = \begin{bmatrix} 1 - \delta \cdot u_k^2 + v_k \\ \beta \cdot v_k \end{bmatrix}. \tag{2.7}$$

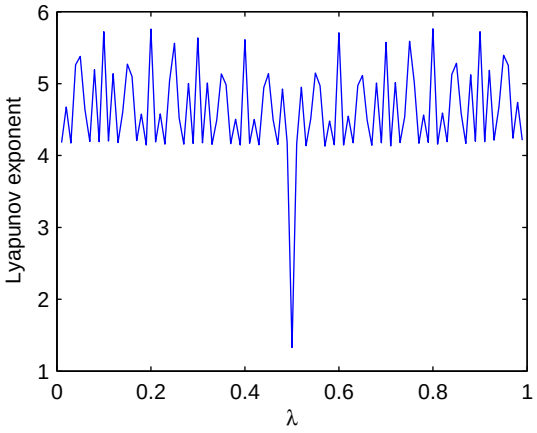
Case study 2.2.1 ([Arroyo08b]). *Cryptanalyis of the cryptosystem proposed in [Chee06]*

In [Chee06] the Hénon map is used as the *heart* of a chaos-based cryptosystem, which entails a security problem that we have highlighted in [Arroyo08b]. In the cryptosystem defined in [Chee06] the plaintext is divided into blocks $\{p_k\}_{k=0}^{N-1}$, where each block has M bits. The encryption of the plain-blocks is carried out for $k = 0 \sim N-1$ in turn. For the k-th plain-block p_k, the corresponding cipher-block is x_{k+1}, which is calculated through Eq. (2.7) by setting

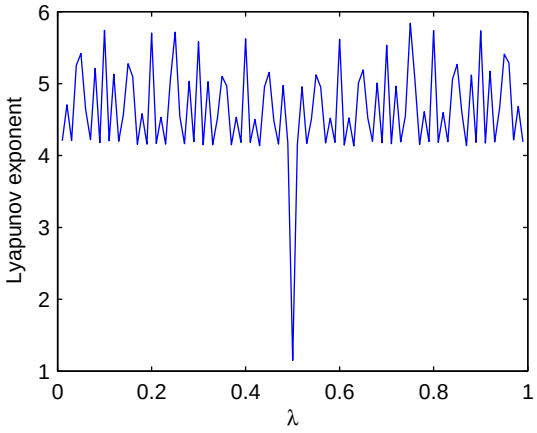
$$\delta = \psi(p_k) \cdot \mu_1(v_k), \tag{2.8}$$

$$\beta = \mu_2(v_k), \tag{2.9}$$

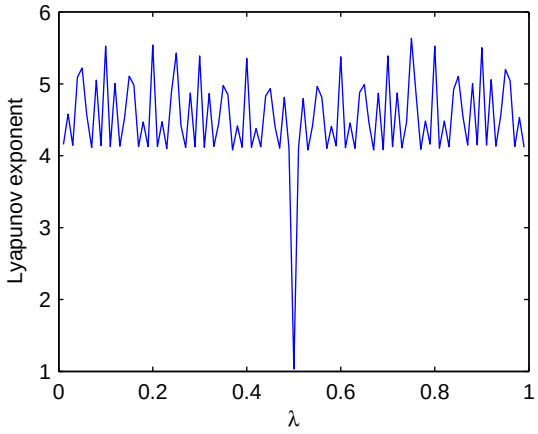
where $\psi(x)$ is a bijective function assuring that δ is a valid parameter of Eq. (2.7)



(a) $\alpha = 33$



(b) $\alpha = 43$



(c) $\alpha = 50$

Figure 2.2: Lyapunov exponent for the discretized version of the skew tent map for different values of the paramenter α.

and $\mu_i(x)$, $i \in \{1, 2\}$, are piecewise linear functions defined as

$$\mu_i(x) = \begin{cases} \beta_{i,1}(x), & \text{if } \delta_{i,1}(x) < |x| \leq \delta_{i,2}(x) \\ \cdots & \cdots \\ \beta_{i,j}(x), & \text{if } \delta_{i,j}(x) < |x| \leq \delta_{i,j+1}(x) \\ \cdots & \cdots \\ \beta_{i,J}(x), & \text{if } \delta_{i,J}(x) < |x| \leq \delta_{i,J+1}(x) \end{cases} \tag{2.10}$$

where $\delta_{i,j}(x)$ is any function making one and only one condition on the right hand of Eq. (2.10) satisfied for any x, and $\beta_{i,j}(x)$ is any function making δ and β valid control parameters of Eq. (2.7). Based on the general form of the proposed cryptosystem, the authors of [Chee06] present a concrete configuration: $M = 48$, $\psi(x)$, $\mu_1(x)$ and

$\mu_2(x)$ are set in Eqs. (2.11), (2.12), (2.13) respectively.

$$\psi(x) = 1.77 \cdot 10^{-2} + 1.39 \cdot 10^{-15} \cdot x, \tag{2.11}$$

$$\mu_1(x) = \begin{cases} 1.27 + \frac{x}{10.2}, & \text{if } |x| \leq 0.1 + \frac{x}{1.3} \\ 1.28 + \frac{x}{10.2}, & \text{if } 0.1 + \frac{x}{1.3} < |x| \leq 0.2 + \frac{x}{1.3} \\ 1.29 + \frac{x}{10.2}, & \text{if } 0.2 + \frac{x}{1.3} < |x| \leq 0.3 + \frac{x}{1.3} \\ 1.30 + \frac{x}{10.2}, & \text{otherwise} \end{cases} \tag{2.12}$$

$$\mu_2(x) = \begin{cases} 0.29 + \frac{x}{10}, & \text{if } |x| \leq 0.1 + \frac{x}{1.1} \\ 0.30 + \frac{x}{10}, & \text{if } 0.1 + \frac{x}{1.1} < |x| \leq 0.2 + \frac{x}{1.1} \\ 0.31 + \frac{x}{10}, & \text{if } 0.2 + \frac{x}{1.1} < |x| \leq 0.3 + \frac{x}{1.1} \\ 0.32 + \frac{x}{10}, & \text{otherwise} \end{cases} \tag{2.13}$$

This configuration does not allow the cryptosystem to work in the chaotic region of the Hénon map, as it was verified through the computation of the maximum LE of the Hénon map. Figure 2.3 depicts the set of points (δ, β) for which the maximal Lyapunov exponent of the Hénon map is positive.

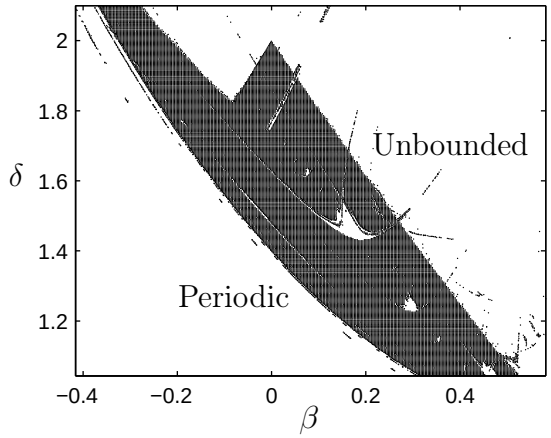
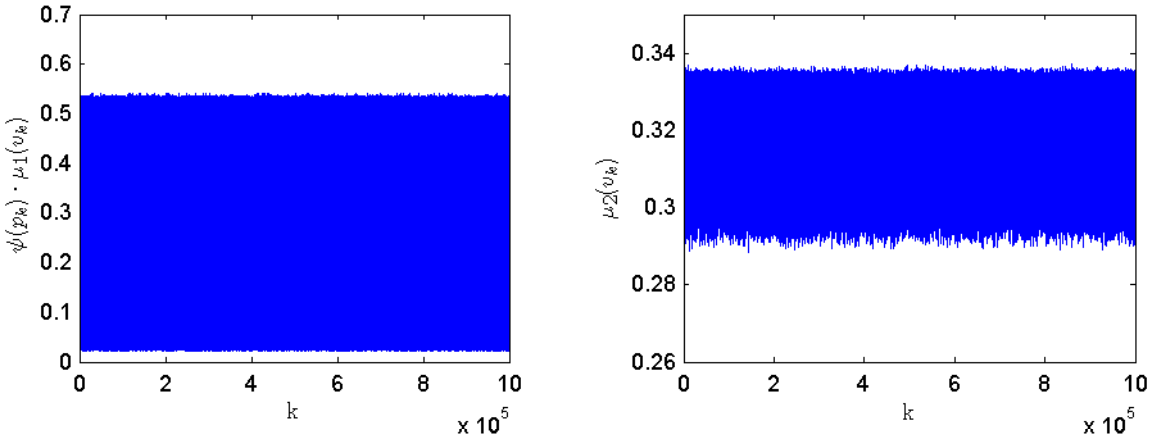


Figure 2.3: Chaotic region for the Hénon map.

When a random plaintext generated by the rand() function of Matlab is encrypted with Eqs. (2.7), (2.11), (2.12), (2.13), $M = 48$, $u_0 = 0.4$ and $v_0 = 0.5$, the product $\psi(p_k) \cdot \mu_1(v_k)$ is always out of the chaotic region (see Fig. 2.4). Figure 2.5 shows that, after a number of transient values, the ciphertext reaches a constant value or a pair of constant values. This is a clear violation of Shannon's requirements for perfect secrecy, since it implies a high value of the conditional entropy (Definition 1.2.3) of the ciphertext with respect to the plaintext. This degradation of the security performance is a result of the cryptosystem being always working in periodic windows of the Hénon



(a) (b)

Figure 2.4: Pseudo-random switching key analysis for the cryptosytem defined in [Chee06]: (a) δ values for random plaintext; (b) β values for random plaintext.

map. The condition for other definitions of $\psi(x)$, $\mu_1(x)$ and $\mu_2(x)$ may be better, but it is difficult to make the system remain always in the chaotic region of the Hénon map. The best solution would be to use other maps with a broader chaotic region.

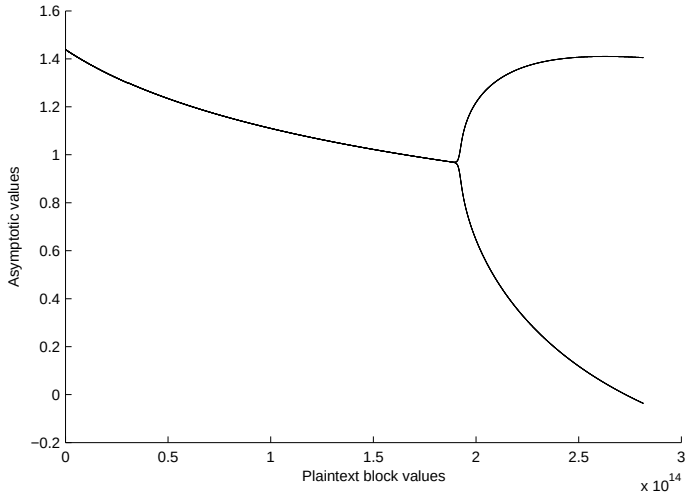


Figure 2.5: Ciphertext values for plaintext blocks with a fixed value when working with the cryptosystem described in [Chee06].

This analysis based on the examination of the LE, must be also done even when the control parameters are design parameters and not part of the key. Indeed, if it is not guaranteed a positive LE for the underlying chaotic system, then a reduction of the level of entropy at the output of the cryptosystem can be observed. For example, in some chaos-based cryptosystems a chaotic map is used as Random Number Generator

(RNG) to select values of the secret key in a random way. If the values of the control parameters do not lead to a positive LE, then a degradation of the chaotic map as RNG is verified, and thus a reduction of the key space (which further implies a decreasing of the conditioned entropy of the output of the cryptosystem with respect to the secret key).

2.3 Analyzing the ergodicity

The ergodic property is a basic requirement for the use of a dynamical system as base of an encryption scheme. Indeed, if a dynamical system is ergodic, the long term behavior of its orbits is independent from the initial condition and can be studied using statistical analysis. This statistical analysis of the long-time behavior is based on the possibility of defining an *invariant measure* for non-conservative ergodic dynamical systems. Given a map $f : \mathcal{U} \to \mathcal{U}$ and $\mathcal{B}$ being σ-algebra over $\mathcal{U}$, μ is an invariant measure of the map if, for each $B \in \mathcal{B}$, it is satisfied

$$\mu(f^{-1}(B)) = \mu(B), \tag{2.14}$$

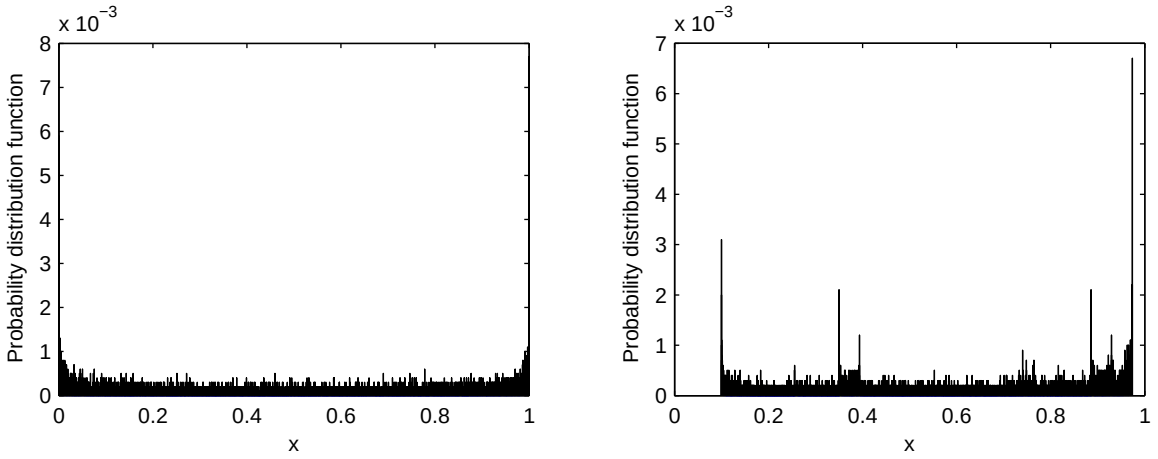
where $f^{-1}(B)$ is the set of preimages of B defined by

$$f^{-1}(B) = \{x \in \mathcal{U} | f(x) \in B\}. \tag{2.15}$$

According to the *ergodic theorem* [Walters82, p. 34], if f is ergodic with respect to the invariant measure μ, then the orbit of $x_0 \in \mathcal{U}$ visits the interval $B \subseteq \mathcal{U}$ with relative frequency $\mu(B)$ for almost all $x_0 \in \mathcal{U}$.

For non-conservative ergodic dynamical systems defined in discrete time, the invariant measure of a map is experimentally approximated through the *histogram* of a long orbit. Let $(f, \mathcal{U}, \Lambda)$ be a discrete-time dynamical system, $\lambda \in \Lambda \subset \mathbb{R}^d$ and $\gamma_{f_\lambda}^M(x_0)$ the first M elements of the orbit derived from the initial condition $x_0 \in \mathcal{U} \subset \mathbb{R}^m$. The histogram associated to $\gamma_{f_\lambda}^M(x_0)$ is calculated upon the partition of $\mathcal{U}$ into N-mutually disjoint subintervals of equal measure. Let $\mathcal{H}_N = \{I_s\}_{s=1}^N$ the considered partition of $\mathcal{U}$ satisfying $\mathcal{U} = I_0 \cup I_1 \cup \ldots \cup I_N$, $I_i \cap I_j = \emptyset$ for all $i \neq j$, and $N << M$. The histogram function is piecewise constant on the partition $\mathcal{H}_N$, and on each subinterval I_s equal to the number of points of $\gamma_{f\lambda}^M(x_0)$ which fall into I_s. At first sight, the calculated histogram depends on N, λ, and x_0. Upon the assumption of ergodicity the dependence on the initial condition does not exist, whereas the dependency on N is eliminated increasing the value of N. Nevertheless, the dependency on λ lies on the dynamical properties of the considered map. In this sense, for some ergodic maps there exists a clear relationship between the shape of the computed histograms and

the value of the control parameters. Considering the case of chaos-based cryptography, this feature must be carefully handled since it could be used by a cryptanalyst to infer the value of the control parameter just analyzing, if possible, the chaotic orbits leading the encryption of information.



(a) (b)

Figure 2.6: Histograms of the logistic map for $M = 100000$, $N = 10000$, and (a)$\lambda = 4$; (b)$\lambda = 3.89472$.

As it is shown in Fig. 2.6, the histogram of the logistic map is dependent on the value of the control parameter. As a matter of fact, the shape and the width of the histogram changes with λ. This is a consequence of logistic map possessing an invariant set depending on the value of λ. Certainly, the function $f_\lambda(x)$ defined by Eq. (1.9) reaches its maximum for $x_c = 1/2$ and, consequently, that function cannot attain a value greater than $\lambda/4$. Furthermore, if λ is such that $LE(\lambda) > 0$, then the minimum value contained in the orbit obtained from x_c is $f_\lambda(\lambda/4) = \frac{\lambda^2}{4}(1-\lambda/4)$. On the other hand, if λ is selected in such a way that the logistic map does not possess periodic stable orbits, then the set of preimages of x_c is dense, i.e., the set

$$\{x | f_\lambda(x) = x_c \text{ for some n} \geq 0\}$$

is dense in $\mathcal{U} = [0, 1]$ [Guckenheimer79]. In other words, for any value x in $\mathcal{U}$, and λ such that $LE(\lambda) > 0$, after a transient number of iterations the orbit derived from x reach the critical point x_c, and all the successive iteration values are inside the interval

$$\left[\frac{\lambda^2}{4}(1-\lambda/4), \lambda/4\right]. \tag{2.16}$$

Case study 2.3.1 ([Arroyo08d]). *Cryptanalysis of the cryptosystem defined in [Pisarchik06]*

A chaos-based image encryption algorithm is defined in [Pisarchik06] using the logistic map. We have cryptanalyzed this cryptosystem in [Arroyo08d], being part of the cryptanalysis based on the property of the logistic map commented just above. In order to explain how that cryptanalysis works, next the cryptosystem defined in [Pisarchik06] is succinctly described. Given an $M \times N$ color image with R, G, B color components, an initialization process is performed to convert the integer values of each pixel to real numbers that can be encrypted using Eq. (2.1), and Eq. (1.9). First, the 2-D image is scanned in the raster order (i.e., from left to right and from top to bottom) to form three 1-D integer sequences $\{P_c^i\}_{i=1}^J$ ($c =$ R, G and B), where $P_c^i \in \{0, \cdots, 255\}$ denotes the color component c of the i-th pixel and $J = M \times N$ (see Fig. 2.7). Then, the integer sequences are converted to three real-number sequences

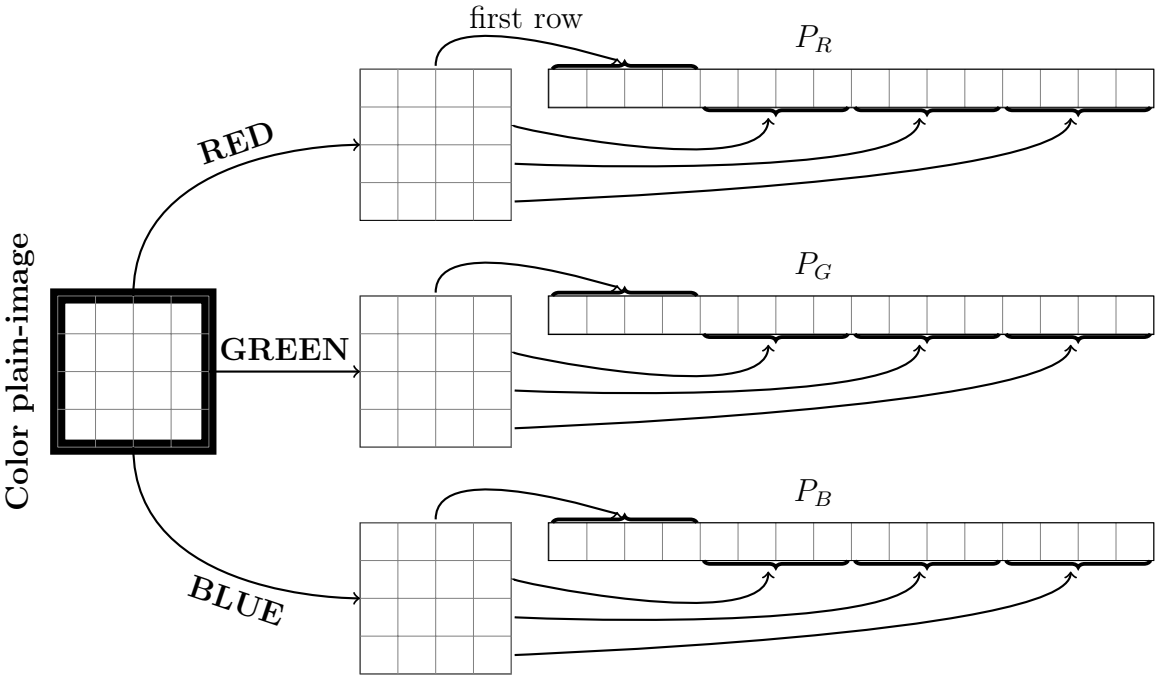


Figure 2.7: Transformation of the color image into three vectors.

each of which corresponds to a different color component: $\{x_c^i(0)\}_{i=1}^J$, where

$$x_c^i(0) = x_{\min} + (x_{\max} - x_{\min}) \cdot P_c^i/255, \tag{2.17}$$

with $x_{min} = \frac{\lambda^2}{4}(1 - \lambda/4)$, and $x_{max} = \lambda/4$. After the above initialization process, the following encryption procedure is carried out separately for each color component to obtain the ciphertext:

1. Set $r = 1$.

2. Set the initial condition of the logistic map as follows:

$$x_0 = \begin{cases} x_c^J(r-1), & \text{if } i = 1 \\ x_c^{i-1}(r), & \text{if } 2 \le i \le J \end{cases}$$

3. Iterate the chaotic logistic map (Eq. 1.9) from x_0 for n times to obtain x_n.

4. Set $x_c^i(r) = x_n + x_c^i(r-1)$. If $x_c^i(r) > x_{\max}$, then subtract $(x_{\max} - x_{\min})$ from $x_c^i(r)$ to ensure $x_c^i(r) \in [x_{\min}, x_{\max}]$.

5. Set $r = r + 1$. If $r < j$, go to Step 2; otherwise the encryption procedure stops for the current color component.

After performing the above encryption procedure for all three color components, the three sequences $\{x_R^i(j)\}_{i=1}^J$, $\{x_G^i(j)\}_{i=1}^J$ and $\{x_B^i(j)\}_{i=1}^J$ make up the ciphertext.

As claimed in [Pisarchik06], the secret key is composed of the following four sub-keys:

1. The control parameter of the logistic map, i.e., λ.

2. The image height and the image width, i.e., M and N respectively.

3. The number of chaotic iterations in Step 3, i.e., n.

4. The number of cycles, i.e., j.

The decryption procedure is similar to the above description, but in an reverse order, and the following inverse map

$$P_c^i = \text{round}[(x_c^i(0) - x_{\min}) \cdot 255/(x_{\max} - x_{\min})] \tag{2.18}$$

is used in the last step to recover the plain-image by converting real numbers back to integer pixel values.

The ciphertext of the cryptosystem proposed in [Pisarchik06] is composed of $3 \cdot J$ real values, each of which is in the range $[x_{\min}, x_{\max}]$. This means that it is possible to approximate $x_{\max}$ as the maximum value of all the real values in the ciphertext, i.e.,

$$\hat{x}_{\max} = \max_{\substack{1 \le i \le J \\ c=\text{R, G, B}}} x_c^i(j). \tag{2.19}$$

Figure 2.8: The plain-image "Lena".

Then, from $x_{\max} \approx \lambda/4$, one can estimate the secret value of the control parameter λ as

$$\lambda \approx \hat{\lambda} = 4 \cdot \hat{x}_{\max}. \tag{2.20}$$

Consequently, if we have a ciphertext, we can estimate the value of the sub-key λ. In other words, a ciphertext-only attack allows us to estimate the sub-key λ. To verify this issue, the image "Lena" (Fig. 2.8) was encrypted for $n = 20$, $j = 1$, and different values of $\lambda \in [3.8, 4]$. These values of λ were then estimated from the ciphertexts by applying Eqs. (2.19) and (2.20). The parameter estimation error (PEE) was calculated as

$$PEE = |\lambda - \hat{\lambda}|, \tag{2.21}$$

for different values of λ that were considered. The PEEs are shown in Fig. 2.9(a). The average estimation error was 5.236228×10^{-6}, whereas the maximum and minimum errors were 3.481322×10^{-5} and 2.758853×10^{-8}, respectively. By increasing the value of j from 1 to 3 and keeping the other sub-keys unchanged, the PEEs are shown in Fig. 2.9(b), being the mean estimation error 4.721420×10^{-6}, the minimum error 1.212016×10^{-8} and the maximum error 3.355227×10^{-5}.

The main conclusion of this analysis is that the ciphertext of a cryptosystem cannot be made up through a sampling process on the orbits of the logistic map. As a matter fact, if the ciphertext is built according to that procedure, then it should be used a chaotic map with invariant set being independent with respect to the control parameters.

The previous analysis does not fully accomplish the evaluation of the "quality" of the ergodicity of chaotic maps in the context of chaos-based cryptography. Indeed, the performance of some encryption architectures requires orbits associated to fixed-

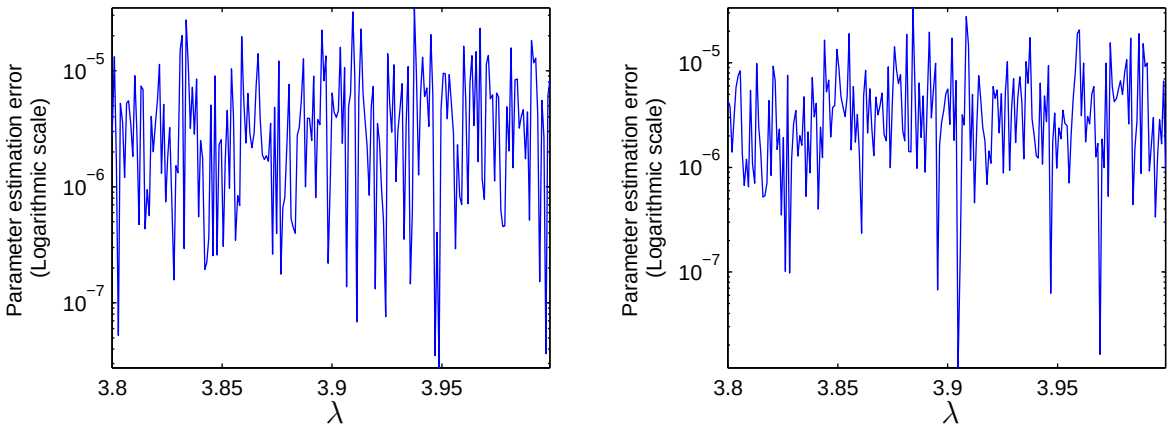


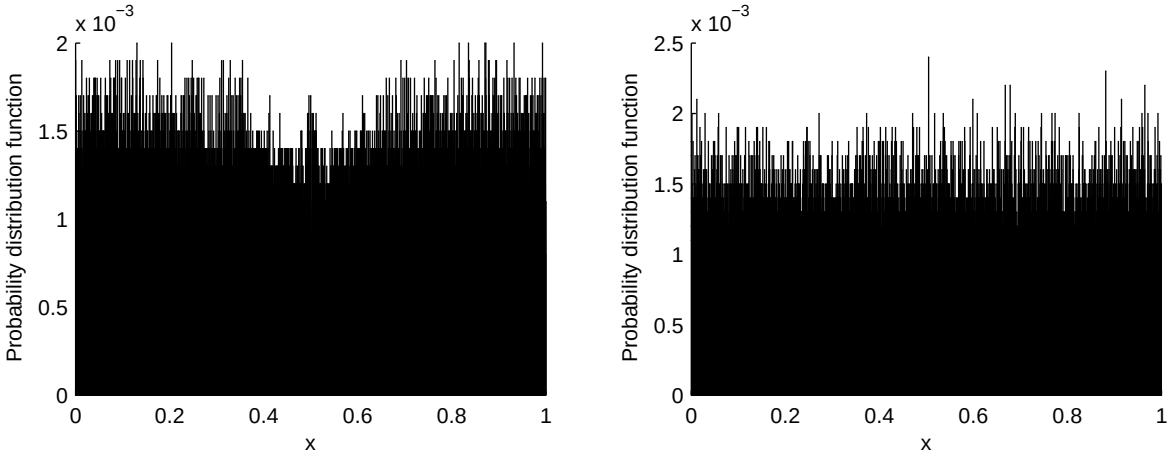
Figure 2.9: Parameter estimation errors corresponding to the image "Lena", when $n = 20$ and (a) $j = 1$; (b) $j = 3$.

width and flat histograms. This is the case of the *searching based chaotic digital ciphers*, as the celebrated Baptista's cryptosytem [Baptista98]. In this type of chaos-based cryptosystem the state space is divided into a number of disjoint intervals given by the cardinality of the alphabet of the plaintext. Upon this setting, the encryption is performed by locating each unit of plaintext in the orbit associated to a certain initial condition. Certainly, each value of the orbit is associated to one of the intervals obtained after partitioning the state space. Starting from last visited interval, we record the number of iterations needed to land into the interval associated to the next unit of plaintext. The number of iterations is the ciphertext corresponding to each unit of plaintext. As a result, the efficiency and security of this kind of cryptosystems demands orbits visiting the different intervals with equal probability. Indeed, if some intervals are visited more frequently than others, then there exists a high correlation between small values of ciphertext and the values of plaintext corresponding to those intervals. In [Baptista98] the logistic map is selected as base of the searching based algorithm. The logistic map possesses a non-flat histogram even when the invariant set occupies the whole space. Indeed, in [Schuster95, p. 68] it is shown that for $\lambda = 4$ the invariant measure of the logistic map is given by

$$\mu(x) = \frac{1}{\pi\sqrt{x(1-x)}}, \tag{2.22}$$

which corresponds to the histogram in Fig. 2.6. A further analysis Fig. 2.6 allows to distinguish an interval of the state space of the logistic map where the histogram is almost flat. Therefore, if it possible to have a flat histogram by locating the

intervals corresponding to the plaintext in a subset of the state space of the logistic map, instead of using the whole state space. Nevertheless, this remedy results in a reduction of the encryption speed. Indeed, most values in the orbits of the logistic map belong to the intervals no associated to plaintext and, consequently, a high number of iterations is necessary to encrypt each unit of plaintext. From this point of view, it is advisable to use maps with a flat histogram, otherwise the efficiency of the designed cryptosystem could be degraded. In this sense, the skew tent map is better option than the logistic map. Certainly, the skew tent map has an invariant measure equal to 1, and thus its associated histogram is flat for any value of the control parameter. Nevertheless, this is a theoretical result that is not confirmed in practice when the



(a) (b)

Figure 2.10: Histograms of the skew tent map for $M = 100000$, $N = 10000$, and (a)$\lambda = 0.01$; (b)$\lambda = 0.4$.

skew tent is implemented using finite precision arithmetics (see Fig. 2.10). As it is explained in [Li03, Chapter 3], finite precision computations cause a degradation of the invariant measure of the skew tent map, which leads to a histogram with a non-flat shape. Consequently, it is not only necessary to use maps with a uniform invariant measure, but also to take into account the consequences of working with finite precision machines.

Up to this point we have shown that the ergodicity of chaotic maps must be evaluated by a deep analysis of the histograms of their orbits. Nevertheless, it is also necessary to perform an additional examination by plotting x_{k+1} versus x_k from a given orbit. This plotting is called *return map*. In Fig. 2.11 the upper and lower bounds of the invariant set of the logistic map are identified through the return map. Either the histogram and return map dependency on the control parameter could imply serious problems when designing a chaos-based cryptosystem. This is case

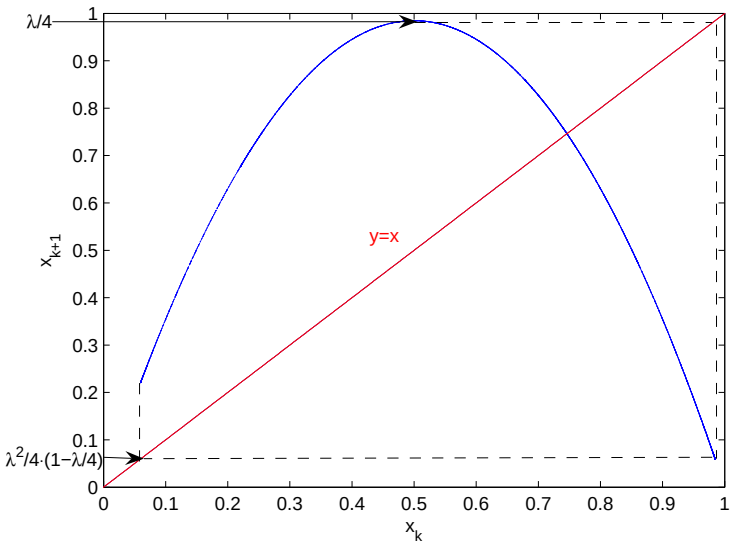


Figure 2.11: Return map of the logistic map for $\lambda = 3.9384739$.

of Baptista's cryptosystem, as it is shown in [Skrobek08]. In that cryptanalytical work the return map of the logistic map is reconstructed through a chosen-ciphertext attack. Once the return map is obtained, the estimation of the control parameter can be done straightforwardly, as Fig. 2.11 informs.

2.4 Measures of entropy

The main reason of the appealing of chaos for cryptographic applications is based on its random-like behavior. Indeed, cryptography is concerned about the concealing of information through its embedding inside of sources 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. In order to establish the limitations and the characteristics of this conditioning, it is necessary to supply a set of mathematical figures.

Assume that $(f, \Lambda, \mathcal{U})$ is a dynamical system in discrete time, with control parameters space $\Lambda \subset \mathbb{R}^d$, state space $\mathcal{U} \subset \mathbb{R}^m$, evolution rule $f_\lambda(x) = f(\lambda, x),\ \forall \lambda \in \Lambda$, and $\mathcal{A} = A_0 \cup A_1 \cup \ldots \cup A_{N-1}$ a finite partition of $\mathcal{U}$. An observation made after k iterations of the map is modeled by the partition $f_\lambda^{-k}(\mathcal{A}) = \left\{f_\lambda^{-k}(A_0), \ldots, f_\lambda^{-k}(A_{N-1})\right\}$, where the k^{th} preimage of $A \subset \mathcal{U}$ is

$$f_\lambda^{-k} = \left\{x \in \mathcal{U} | f_\lambda^k(x) \in A\right\}.$$

If f_λ has μ as invariant measure, then the probability of visiting the interval A_i is

$$pr_i = \mu(A_i), i = 1, \ldots, N, \tag{2.23}$$

and the Shannon entropy of the partition $\mathcal{A}$ is

$$H(\mathcal{A}) = -\sum_{i=0}^{N} pr_i \log pr_i. \tag{2.24}$$

The joint distribution of M successive observations is performed by the mutual refinement

$$\mathcal{A}_M = \mathcal{A} \vee f_\lambda^{-1}(\mathcal{A}) \vee \ldots \vee f_\lambda^{-M+1}(\mathcal{A}). \tag{2.25}$$

If $\mathcal{A}$ is built properly, then the upper bound of the entropy of the successive refinements leads to the actual entropy of the chaotic map. This happens when $\mathcal{A}$ is a *generating partition.*

Definition 2.4.1 (Generating partition)**.** *Let $(f, \Lambda, \mathcal{U})$ a discrete-time dynamical system, with control parameters space $\Lambda \subset \mathbb{R}^d$, state space $\mathcal{U} \subset \mathbb{R}^m$, evolution rule $f_\lambda(x) = f(\lambda, x),\ \forall \lambda \in \Lambda$, and $\mathcal{A}$ a partition of its state space. If it is satisfied the following equation*

$$H(f_\lambda, \mathcal{A}) = \lim_{M \to \infty} \frac{1}{M} H(\mathcal{A}_M), \tag{2.26}$$

then $\mathcal{A}$ is a generating partition of the considered dynamical system.

Shannon entropy is also known as Shannon-Boltzmann-Gibbs measure of entropy, and it provides a good characterization of the entropy of systems involving correlations of short distance, markovian systems, and, in general, systems that possess a robust chaotic microscopic dynamic, i.e., a dynamic with strictly positive Lyapunov exponent and full ergodic behavior through the complete phase space. However, Shannon-Boltzmann-Gibbs' characterization fails in the description of those systems with a weak chaotic behaviour in a microscopic scale, which implies a Lyapunov spectrum with zero-crossings. The temporal evolution of these systems does not cover the complete phase space but a subregion of it with (multi)fractal or hierarchical structure. Therefore, it is necessary to use a non-extensive examination of the dynamics to achieve a more accurate characterization of those kind of dynamical systems. Taking into account these needs, in 1988 Tsallis proposed a generalization of the Shannon-Boltzmann-Gibbs measure of entropy [Tsallis88]. According to Tsallis' criterion, the entropy of a partition $\mathcal{A}$ can be calculated as

$$H_{TS}(\mathcal{A}, q) = \frac{1}{q-1} \sum_{j=1}^{N} \left(pr_j - (pr_j)^q \right), \tag{2.27}$$

where $q \in \mathbb{R}$.

Independently of the specific method to calculate the entropy, a crucial stage of the entropy analysis is to find a generating partition. Different methods have been proposed based on the Fourier analysis [Powell79], the Wavelet transform [Rosso02], histograms [Martin06] or the permutation entropy [Bandt02]. A very useful tool for either the determination of generating partition or the computation of different figures of entropy is the theory of *symbolic dynamics*.

Definition 2.4.2 (Symbolic dynamics)**.** *Let $\mathcal{A} = \{A_0, A_1, \ldots, A_{n-1}\}$ a partition of $\mathcal{U} \subset \mathbb{R}$ satisfying that $\mathcal{U} = \cup_{i=0}^{n-1} A_i$ and $A_i \cap A_j = \emptyset$ for $i \neq j$. If $n = 1$ the partition is called trivial. For a partition $\mathcal{A}$, a unique symbol $i = \theta(A_i)$ is assigned to every region $A_i \in \mathcal{A}$. The process of partitioning $\mathcal{U}$, assigning symbols to every region of the partition, and the resulting macroscopic dynamics are called* symbolic dynamics.

For the class of maps in $\mathcal{F}$, the theory of symbolic dynamics leads straightforwardly to a generating partition. Indeed, when considering unimodal maps, the value of the critical point x_c divides $\mathcal{U}$ into two subintervals, which further determines a generating partition. In this sense, any orbit of a unimodal map can be translated into a sequence of 0-bits and 1-bits (a value x_i of an orbit is assigned to a 0-bit/1-bit if $x_i < x_c / x_i \geq x_c$). The analysis of the dynamics of unimodal maps by means of their symbolic dynamics is very fruitful, as will be explained in Chapter 3, and it also allows the determination of measures of entropy.

As it is pointed out in [Ebeling92], symbolic sequences can be used to build an approximation of the entropy of the underlying dynamical system. However, this approximation is not done on the symbols included in symbolic sequences, but on groups of those symbols. Indeed, subgroups of n symbols or letters are determined from any symbolic sequence, and the number of occurrences of each of the possible *n-words* are computed. If the considered dynamical system is chaotic, then it can be assumed stationarity. In this situation, $pr_i^{(n)}$ is the probability of occurrence of the word i, among the J^n possible words, being J the cardinality of the alphabet used in the symbolic dynamics of the dynamical system. Following Shannon, *n-gram* entropies are given by

$$H_n = -\sum_{i=1}^{J^n} pr_i^{(n)} \log pr_i^{(n)}. \tag{2.28}$$

Furthermore, the entropy H_n can be later used to calculate the average information necessary to predict the next symbol given the preceding n symbols. This measure is called *n-gram conditional entropy*, noted as h_n, and defined mathematically as

$$h_n = H_{n+1} - H_n, \tag{2.29}$$

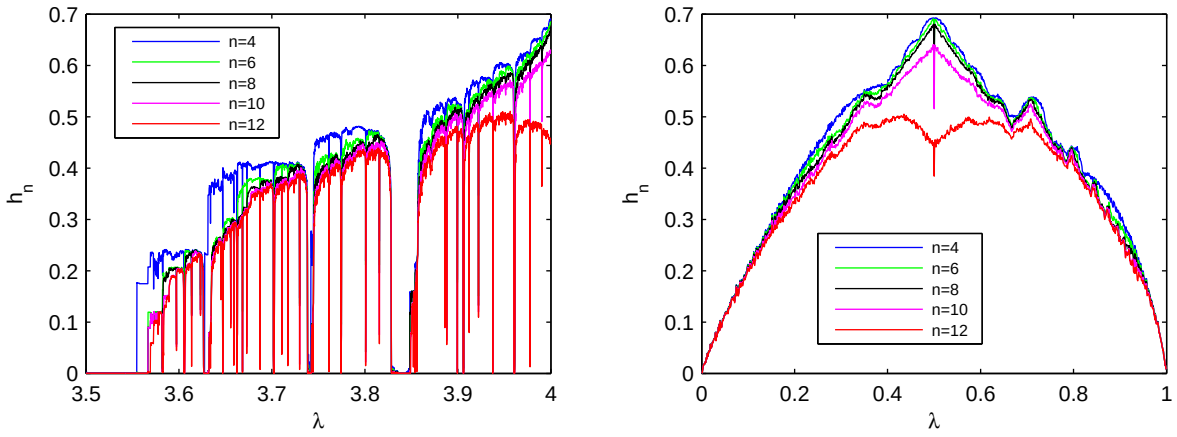
where $h_0 = H_1$. The previous definition implies that

$$h_{n+1} \leq h_n, \tag{2.30}$$

and that the entropy of the considered generating partition $\mathcal{A}$ is given by the limit of the conditional entropies, i.e.,

$$H(\mathcal{A}) = \lim_{n\to\infty} h_n = \lim_{n\to\infty} \frac{H_n}{n}. \tag{2.31}$$

In Fig. 2.12 it is shown the varying of the n-gram conditional entropy with respect to the word length for the logistic and skew tent map. Simulation results confirm what was expected from theory, i.e., the n-gram conditional entropy can be used to establish the chaoticity of a symbolic sequence and as alternative to the Lyapunov exponent. Indeed, Fig. 2.12 and Fig. 2.1 spell out that it is possible to establish a threshold for the n-gram conditional entropy such that a larger value implies chaos. Furthermore, in the case of the skew tent map the conditional entropy pinpoints a two-to-one relation with respect to the control parameter. This relation is also present in the Lyapunov exponent, but the computation of the conditional entropy is less computationally demanding, and also can be calculated from both the exact orbits and the symbolic sequences.



(a) (b)

Figure 2.12: n-gram conditional entropy of the logistic map (a) and skew tent map (b) for different values of the word length.

2.5 Time-frequency characterization of chaotic sequences

In information theory the standard methodology when dealing with the temporal evolution of systems is mostly based on the Fourier transform. Indeed, the projection of a signal or sequence on the frequencies domain can lead to meaningful conclusions about its periodical or non-periodical behavior. In the case of a system defined in discrete time the tool to use is the *Discrete Fourier Transform* or *DFT* . However, the DFT determines a total characterization of a sequence of values if it is the counterpart of the temporal evolution of a system with a stationary behavior. This is not the case of chaotic systems. Certainly, the counterpart of a chaotic system in the frequencies domain is not constant, it is time dependant. In this sense, if a given chaotic sequence is split into several disjoint chaotic subsequences, the DFT of each of those subsequences are sensibly different from each other. Therefore, it is necessary to establish another way of registering both the behavior in the frequencies domain and the modification with time of this behavior. In other words, it is necessary to perform a time-frequency characterization of chaotic systems. The *Wavelet Transform* or *WT* is the tool leading the analysis of the time-frequency description of systems with non-stationary temporal evolution.

The *Continuous Wavelet Transform* (*CWT*) of a continuous signal $x(t)$ is

$$Wx(u,s) = \langle x, \psi_{u,s} \rangle = \int_{-\infty}^{+\infty} x(t) \frac{1}{\sqrt{s}} \psi^* \left(\frac{t-u}{s} \right) dt, \tag{2.32}$$

where $\psi_{u,s}(t) = \psi(\frac{t-u}{s})$. If $s = 2^{-j}$, $u = k \cdot 2^{-j}$ for $j,\ k \in \mathbb{N}$, then we have a *Dyadic Wavelet Transform* or *DWT*. The DWT employs a set of windows whose size is variable and proportional to 2^{-j} in order to extract information about the data structure for different scales. This transform can be inverted and the original signal recovered if $\psi(t)$ satisfies certain properties [Mallat99]. There is an special type of DWTs that can be implemented using very efficient algorithms [Mallat89]. Those algorithms are based on mathematical structures called multiresolution approximations of $L^2(\mathbb{R})$ (the space of real square summable functions). A sequence $\{\mathcal{V}_j\}_{j \in \mathbb{Z}}$ of closed subspaces of

$L^2(\mathbb{R})$ is a multiresolution approximation if the following properties are satisfied:

$$\forall (j,k) \in \mathbb{Z}^2, f(t) \in \mathcal{V}_j \Leftrightarrow f(t-2^j k) \in \mathcal{V}_j, \tag{2.33}$$

$$\forall j \in \mathbb{Z}, \mathcal{V}_{j+1} \subset \mathcal{V}_j, \tag{2.34}$$

$$\forall j \in \mathbb{Z}, f(t) \in \mathcal{V} \Leftrightarrow f\left(\frac{t}{2}\right) \in \mathcal{V}_{j+1}, \tag{2.35}$$

$$\lim_{j \to +\infty} \mathcal{V}_j = \bigcap_{j=-\infty}^{+\infty} \mathcal{V}_j = \{0\}, \tag{2.36}$$

$$\lim_{j \to -\infty} \mathcal{V}_j = \text{Closure}\left(\bigcup_{j=-\infty}^{+\infty} \mathcal{V}_j\right) = L^2(\mathbb{R}). \tag{2.37}$$

The goal is to obtain a sequence of successive approximations of the original signal through its reiterative projections on subspaces $\mathcal{V}_j$ of $L^2(\mathbb{R})$. These subspaces are generated by the scaling function $\phi(t)$:

$$\mathcal{V}_j = \left\{ \sum_{k \in \mathbb{Z}} c_j(k) \phi_{j,k}(t) \right\}, \tag{2.38}$$

where $\phi_{j,k}(t) = 2^{j/2}\phi(2^j t - k)$ are dilations (or reductions) and translations in time of the function $\phi(t)$. It is also necessary that $\{\phi_{j,k}(t), k \in \mathbb{Z}\}$ is an unconditional base of $\mathcal{V}_j$. Consequently, the multiresolution approximation can be interpreted as an "stair" of spaces embedded one into another. As conditions (2.33)-(2.37) inform, the scaling function $\phi(t)$ can not be selected arbitrarily. Since $\mathcal{V}_1 \subset \mathcal{V}_0$, $2^{1/2}\phi(t/2) \in \mathcal{V}_1$ and $\phi(t) \in \mathcal{V}_0$, and having under consideration that $\{\phi(t-n)\}_{n \in \mathcal{Z}}$ is an orthonormal base of $\mathcal{V}_0$, it is possible to express

$$\frac{1}{\sqrt{2}}\phi\left(\frac{t}{2}\right) = \sum_{n=-\infty}^{+\infty} h[n]\phi(t-n), \tag{2.39}$$

with

$$h[n] = \left\langle \frac{1}{\sqrt{2}}\phi\left(\frac{t}{2}\right), \phi(t-n) \right\rangle. \tag{2.40}$$

Applying the Fourier transform in both sides of Eq.(2.39), we have

$$\Phi(2\omega) = \frac{1}{\sqrt{2}} H(\omega)\Phi(\omega). \tag{2.41}$$

For $p \geq 0$, the previous equation can be generalized as

$$\Phi(2^{-p+1}\omega) = \frac{1}{\sqrt{2}} H(2^{-p}\omega)\Phi(2^{-p}\omega), \tag{2.42}$$

which further leads to

$$\Phi(\omega) = \left(\prod_{p=1}^{P} \frac{H(2^{-p}\omega)}{\sqrt{2}} \right) \Phi(2^{-P}\omega). \tag{2.43}$$

If $\Phi(\omega)$ is continuous for $\omega = 0$, the $\lim_{P \to +\infty} \Phi(2^{-P}\omega) = \Phi(0)$, and consequently it is satisfied the following equation:

$$\Phi(\omega) = \prod_{p=1}^{+\infty} \frac{H(2^{-p}\omega)}{\sqrt{2}} \Phi(0). \tag{2.44}$$

The next theorem gives the necessary and sufficient conditions that $H(\omega)$ must satisfy to make Eq.(2.44) the Fourier transform of the scaling function.

Theorem 2.5.1 ([Mallat89]). *Let $\phi \in L^2(\mathbb{R})$ be an integrable scaling function. The Fourier transform of $h[n] = \left\langle 2^{-1/2}\phi(t(2), \phi(t-n) \right\rangle$ satisfies*

$$\forall \omega \in \mathbb{R}, |H(\omega)|^2 + |H(\omega + \pi)|^2 = 2, \tag{2.45}$$

and

$$H(0) = \sqrt{2}. \tag{2.46}$$

On the other hand, if $H(\omega)$ is 2π-periodic and continuous differentiable in a neighborhood of $\omega = 0$, and Eq.(2.45) and Eq.(2.46) are satisfied along with the following condition

$$\inf_{\omega \in [-\pi/2, \pi/2]} |H(\omega)| > 0, \tag{2.47}$$

then the Fourier transform of the scaling function $\phi \in L^2(\mathbb{R})$ is

$$\Phi(\omega) = \prod_{p=1}^{+\infty} \frac{H(2^{-p}\omega)}{\sqrt{2}}. \tag{2.48}$$

The discrete filters satisfying Eq.(2.45) are called *conjugate filters*. The approximations of $x(t)$ in the scales 2^j and 2^{j-1} are, respectively, its orthogonal projection over $\mathcal{V}_j$ and $\mathcal{V}_{j-1}$. Let us call $\mathcal{W}_j$ the orthogonal complement of $\mathcal{V}_j$ in $\mathcal{V}_{j-1}$:

$$\mathcal{V}_{j-1} = \mathcal{V}_j \oplus \mathcal{W}_j. \tag{2.49}$$

The orthogonal projection of $x(t)$ on $\mathcal{V}_{j-1}$ can be expressed as the sum of the orthogonal projections over $\mathcal{V}_j$ and $\mathcal{W}_j$:

$$P_{\mathcal{V}_{j-1}} x = P_{\mathcal{V}_j} x + P_{\mathcal{W}_j} x \tag{2.50}$$

Since the projection onto $\mathcal{V}_j$ represents the approximation at the scale 2^j, the projection onto the complementary subspace $\mathcal{W}_j$ entails the details of the signal $x(t)$ at the scale 2^j, but not at the scale 2^{j-1}. The next theorem shows that it is possible to build a base of $\mathcal{W}_j$ by scaling and translating the wavelet function ψ.

Theorem 2.5.2 ([Mallat89]). *Let ϕ be an scaling function and $h[n]$ the associated conjugate mirror filter. Let ψ be the function with Fourier transform given by*

$$\Psi(\omega) = \frac{1}{\sqrt{2}} G\left(\frac{\omega}{2}\right) \Phi\left(\frac{\omega}{\sqrt{2}}\right), \tag{2.51}$$

where $G(\omega)$ is defined as:

$$G(\omega) = e^{i\omega} H^*(\omega + \pi). \tag{2.52}$$

Let us defined the set of functions $\psi_{j,k}(t)$ as

$$\psi_{j,k}(t) = \frac{1}{\sqrt{2^j}} \psi\left(\frac{t - 2^j k}{2^j}\right). \tag{2.53}$$

For any scale 2^j, $\{\psi_{j,k}\}_{k\in\mathbb{Z}}$ is an orthonormal basis of $\mathcal{W}_j$. For all the scales, $\{\psi_{j,k}\}_{(j,k)\in\mathbb{Z}^2}$ is an orthonormal base of $L^2(\mathbb{R})$.

The proof of Theorem 2.5.1 and Theorem 2.5.2 can be found in [Mallat99], where it is also shown that $G(\omega)$ is the Fourier transform of

$$g[n] = \left\langle \frac{1}{\sqrt{2}} \psi\left(\frac{t}{2}\right), \phi(t - k) \right\rangle, \tag{2.54}$$

which are the decomposition coefficients of

$$\frac{1}{\sqrt{2}} \psi\left(\frac{t}{2}\right) = \sum_{k=-\infty}^{+\infty} g[k] \phi(t - k). \tag{2.55}$$

The orthogonal projections of a signal $x(t)$ on the consecutive "detail" subspaces $\mathcal{W}_j$ are obtained with a partial expansion in its wavelet basis

$$P_{\mathcal{W}_j} x = \sum_{k=-\infty}^{+\infty} \langle x, \psi_{j,k} \rangle \, \psi_{j,k}. \tag{2.56}$$

The expansion of a signal in an orthogonal wavelet basis can be interpreted as a multiresolution approximation at the different scales 2^j, i.e.,

$$x = \sum_{j=-\infty}^{+\infty} P_{\mathcal{W}_j} x = \sum_{j=-\infty}^{+\infty} \sum_{k=-\infty}^{+\infty} \langle x, \psi_{j,k} \rangle \, \psi_{j,k}. \tag{2.57}$$

Finally, and before continuing with the application of the multiresolution analysis of chaos, it is necessary to make an observation with respect to the selection of the orthonormal basis $\{\psi_{j,k}\}_{(j,k)}$. Although Theorem 2.5.2 makes explicit the conditions that $\phi(\omega)$ must satisfy to determine $\{\psi_{j,k}\}_{(j,k)}$ as an orthonormal basis in $L^2(\mathbb{R})$, it

does not prove that an orthonormal basis is the sustain of a multiresolution approximation. Nevertheless, in [Lemarié90] it is proved that $\psi(\omega)$ with compact support and satisfying Theorem 2.5.2 leads to multiresolution approximations of signals. In [Gamero97; Rosso01] it is used a function $\Psi(\omega)$ with the requirements pointed out in [Lemarié90]. Precisely, in those works a Battle-Lemarié wavelet function of order 3 is used. Henceforth, it is assumed that all the analysis are performed with this wavelet function.

2.5.1 Wavelet entropy

The decomposition of a signal into the different resolution levels defined by the orthonormal basis $\psi_{j,k}$ is a *multiresolution analysis* or *MRA*. The MRA of a signal allows a discretization of the original signal by means of the energy associated to each resolution level. Let S be a set of M elements obtained by sampling a signal $s(t)$ at a sample rate of T_s seconds ($S = \{s(0), s(T_s),\ \ldots,\ s((M-1)T_s)\}$). If the wavelet coefficients of S are

$$C_j(k) = \langle S, \psi_{j,k} \rangle \,, \tag{2.58}$$

the energy associated to each resolution level E_j is

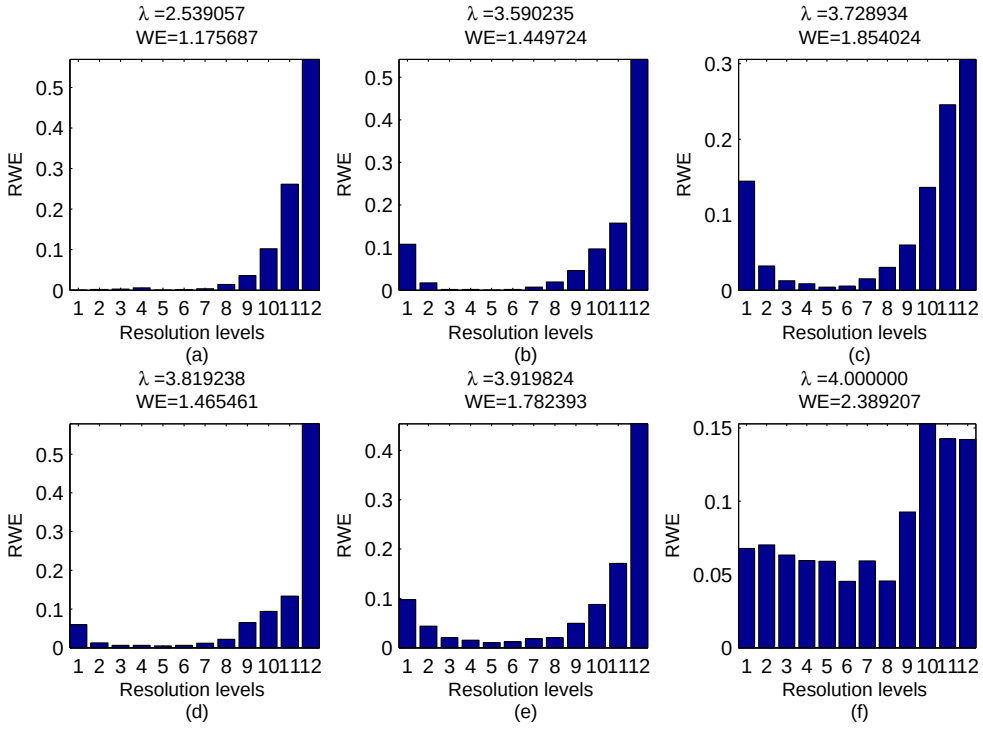


Figure 2.13: RWE of the logistic map for different values of the control parameter.

$$E_j = \frac{1}{N_j} \sum_k |C_j(k)|^2, \tag{2.59}$$

being N_j the number of coefficients at scale j ($j = 1,\ 2,\ \ldots,\ N$ and $N = \log_2(M)$). The total energy is determined as

$$E_{tot} = ||S||^2 = \sum_{j<0} \sum_k |C_j(k)|^2 = \sum_{j<0} E_j, \tag{2.60}$$

whereas the *Relative Wavelet Energy* or of each resolution level is defined as the ratio between the energy associated to each scale and the total energy, i.e.,

$$RWE_j = \frac{E_j}{E_{tot}}, \tag{2.61}$$

for $j = 1,\ 2, \ldots, N$. The RWE is a very useful to conclude if a given sequence of values can be considered as a good source of entropy. Certainly, the RWE satisfies $\sum_j RWE_j = 1$ and can be interpreted as the probability distribution function of the energy. Based on this concept, the *Wavelet Entropy* or *WE* is defined as

$$WE = -\sum_{j<0} RWE_j \ln RWE_j. \tag{2.62}$$

A dynamical system is a good source of entropy if all the resolution levels of the multiresolution analysis possess the same energy. In this case, the WE is maximum and the associated dynamical system can be considered chaotic in the strict sense. In Figs. 2.13 and 2.14 the RWE is depicted for different values of the control parameter of the logistic and the skew tent map, respectively.

Both figures show how the WE increases as the differences between the energy of resolution levels decreases. In the case of the logistic map the values of λ determining periodic behavior are easily identified by means of low values of WE and a RWE with most components equal to zero, with the exception of those components associated to one or several resolution levels. The skew tent map, in turn, possesses a RWE with a better distribution of energy among the different levels. Nevertheless, even in the case of the skew tent map the WE is not maximum, since the distribution of energy between resolution levels in not strictly equitable. Certainly, there always exists outstanding resolution levels in the "sharing", being specially relevant the situation defined by values of λ close to either 0 or 1.

In [Torres00; Rosso01; Rosso02] the WE is not only introduced as a measure of order in a signal, but as an alternative to other features as the Lyapunov exponent, correlation dimensions and the Hurst exponent. In Fig. 2.15 the WE of the logistic map is shown, whereas the WE of the skew tent map is shown in Fig. 2.16. In both

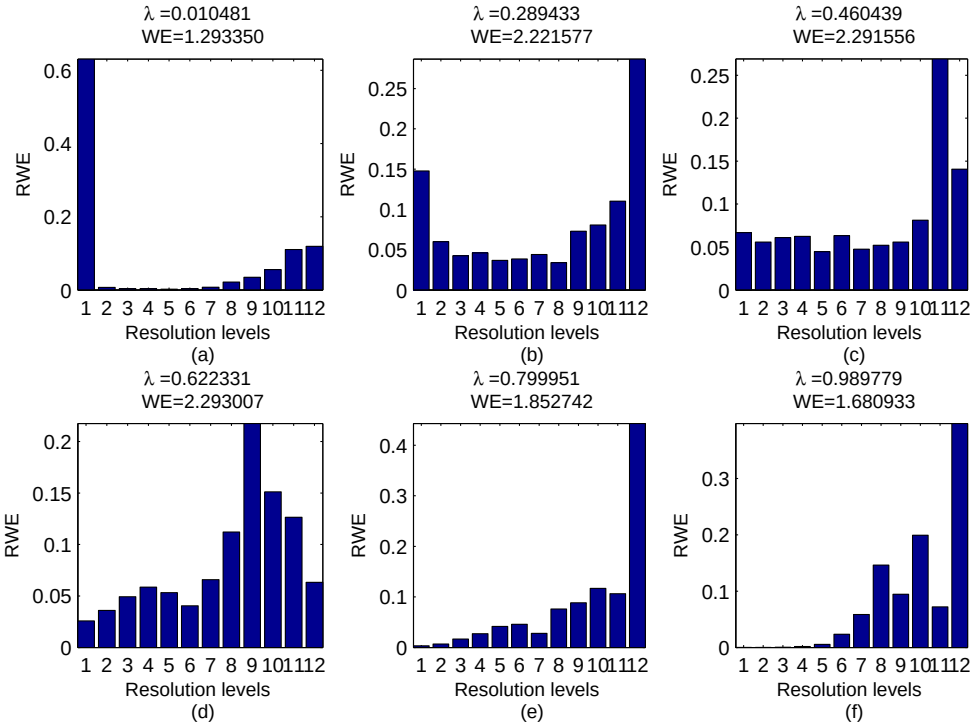


Figure 2.14: RWE of the skew tent map for different values of the control parameter.

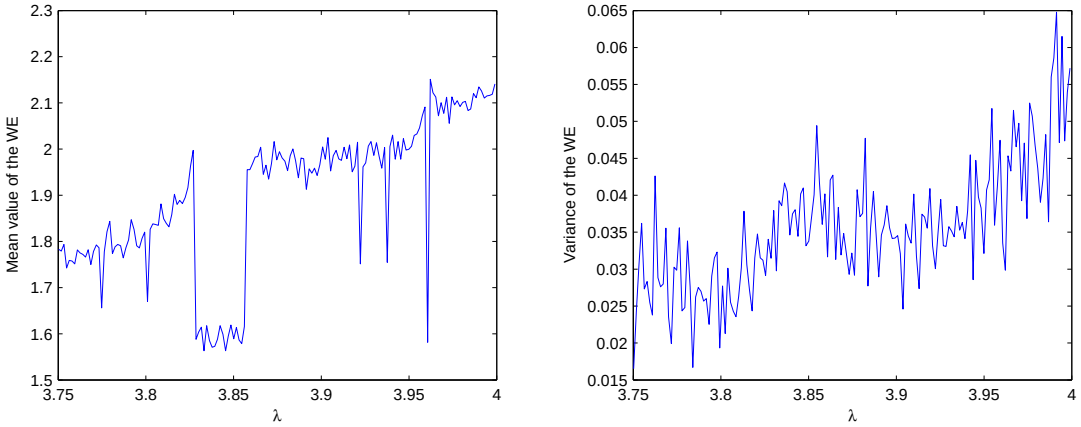
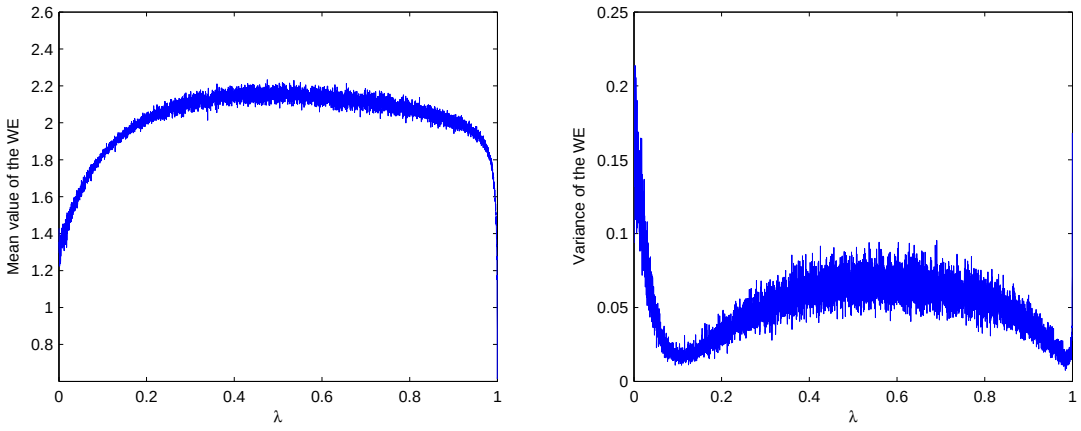


Figure 2.15: WE of the logistic map for different values of the control parameter.

cases the WE can be interpreted as a criterium to establish the chaoticity of a given time series, although it has to be handled carefully since its value fluctuates with the initial condition. Nevertheless, the WE offers a parameter free method to measure order with a lower computational burden and a higher immunity against noise, due to the filtering made by the wavelet transform. In this sense, the WE must be considered as a basic tool for cryptanalysis of chaos-based cryptosystems.



(a) (b)

Figure 2.16: WE of the skew tent map for different values of the control parameter.

2.5.2 Multiresolution entropy

In the previous section the Battle-Lemarié wavelet function of order 3 has been proposed as the sustain of a method to compute the entropy of a giving sequence of values. Nevertheless, not only that type of wavelet function is useful in the analysis of chaotic systems. In [Gamero97] cubic spline wavelet functions are used to build another measure of entropy. In this case, the DWT coefficients of a given sequence S, i.e., $C_j(k) = \langle S, \psi_{j,k} \rangle$ are transformed using an *sliding window*. The sliding window of the resolution level j is given by

$$W_j(u, w, \Delta) = \{C_j(k), k = 1 + u \cdot \Delta, 2 + u \cdot \Delta, \ldots, w + u \cdot \Delta\}\,, \tag{2.63}$$

where $w \leq K_j$ is the width of the sliding window and Δ is selected satisfying $(K_j - w)/\Delta \in \mathbb{N}$, being K_j the number of wavelet coefficients at the resolution level j. Next the sliding window is used to define the *MultiResolution Entropy* or *MRE*.

Definition 2.5.1 (MRE)**.** *Let $C_{min,j}$ and $C_{max,j}$ be the minimum and maximum values of the coefficients $C_j(k)$ included in $W_j(u, w, \Delta)$. The interval $[C_{mix,\,j}, C_{max,\,j}]$ is divided into the following $J \in \mathbb{N}$ subintervals of size $t = \lfloor [C_{mix,\,j}, C_{max,\,j}]/J \rfloor$:*

$$\begin{aligned} I_{u,j,1} &= [C_{min}, C_{min} + t)\ , \\ I_{u,j,2} &= [C_{min} + t, C_{min} + 2 \cdot t)\ , \\ &\ldots \\ I_{u,j,J} &= [C_{min} + (J-1) \cdot t, C_{max}]\ . \end{aligned} \tag{2.64}$$

These subintervals are used to calculate a probability distribution function. In this sense, $pr(I_{u,\,j,l})$ is the probability of finding a wavelet coefficient in the interval $I_{u,\,j,l}$.

According to this distribution function, the MRE can be calculated. If the MRE is determined accordingly, then it is noted as $MRES_j$ (MRE in the sense of Shannon at the resolution level j), whereas in case of choosing Tsallis' criterium it is noted as $MRET_j$.

As it is emphasized in [Gamero97] the main application of the MRE is the detection of changes in the entropy of temporal series. In the context of chaos-based cryptography this detection could be useful to infer some information about the plaintext or to build some mechanism to estimate either the control parameters or the initial condition. As a result, the MRE should be considered as another auxiliary tool in either the design or the cryptanalysis of a chaos-based cryptosystem. As an example of the virtues of the MRE, let us consider the logistic map with control parameter $\lambda = 3.8123$ and with control parameter changing according to the rule

$$\lambda_n = \begin{cases} \lambda_1, & if\ n < n_1 \\ \lambda_1 + [(n - n_1)(\lambda_2 - \lambda_1)/(n_2 - n_1)], & if\ n_1 \leq n \leq n_2 \\ \lambda_2, & if\ n > n_2 \end{cases} \tag{2.65}$$

where $\lambda_1 = 3.5$, $\lambda_2 = 3.8123$, $n_1 = 1182$, and $n_2 = 1634$.

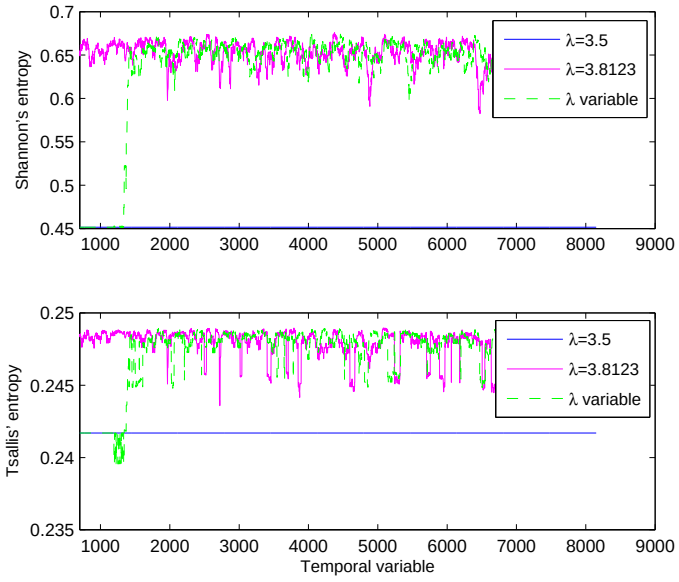


Figure 2.17: Entropy analysis of the logistic map for constant and variable control parameter. The entropy has been computed with $w = 82$, $\Delta = 2$, $J = 5$, and $q = 5$ for Tsallis' entropy.

In Fig. 2.17 the entropy is analyzed just using the sliding window, whereas in Figs. 2.18 and 2.19 the sliding window and the DWT are combined to examine

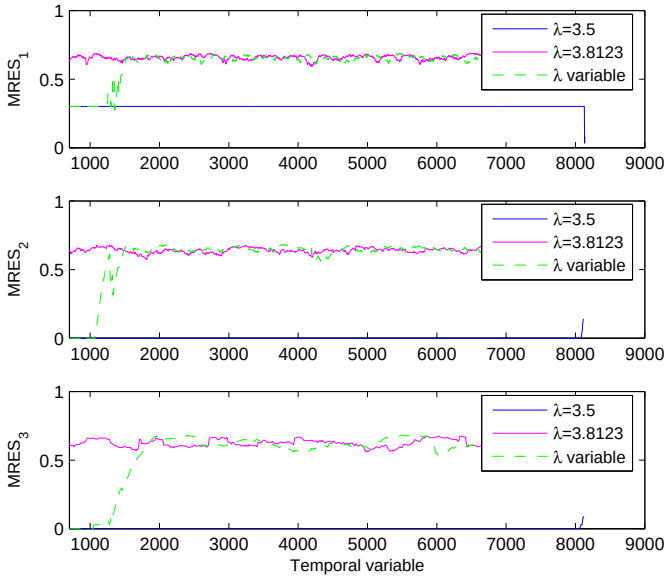


Figure 2.18: Mutiresolution entropy analysis by in the sense of Shannon for the logistic map with constant and variable control parameter. The entropy has been computed with $w = 82$, $\Delta = 2$, and $J = 5$.

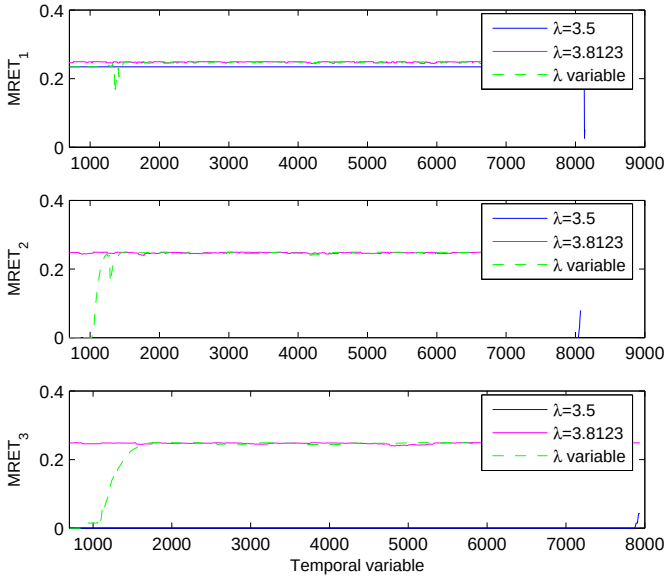


Figure 2.19: Mutiresolution entropy analysis by in the sense of Tsallis for the logistic map with constant and variable control parameter. The entropy has been computed with $w = 82$, $\Delta = 2$, $J = 5$, and $q = 5$.

the entropy according to Shannon's and Tsallis' measures, respectively. In all the

situations it is clearly established the possibility of locating in time the change in the entropy of the system. Nevertheless, it is also possible to locate that change in the frequencies domain by means of the MRE, as Figs. 2.18 and 2.19 shown.

From the point of view of chaos-based cryptography, the possibility of the analysis performed by the MRE is useful when deciding how to use the entropy derived from chaos to conceal information. Indeed, if we want to encrypt information with an spectral behavior clearly located at a certain range of frequency scales, then it is advisable to use a chaotic map with a high level of entropy at those scales. Furthermore, the possibility of locating in time and in frequency the changes of entropy could represent a security flaw. Certainly, if it is possible to establish a relation between values of the control parameters and levels of entropy at the different scales, then the MRE could be used to reduce the key space for a further brute force attack. Another security flaw arises when the entropy of the ciphertext at any frequency scale is influenced by the plaintext. In this case, the MRE of a given ciphertext could lead to a subgroup of plaintexts, which could also be used to reduce the complexity of a brute force attack.

2.6 Study of the sensitivity to control parameter

One characteristic of chaotic systems is that their evolution in time is very dependent on the vector of control parameters. In this sense, two very close values of λ lead to very different instant values of orbits (after a transient number of iterations). Nevertheless, this difference can 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 with respect to the control parameters. Certainly, 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. For a chaotic map $f_\lambda : \mathcal{U} \to \mathcal{U}$ and a generating partition $\mathcal{A} = A_0 \cup A_1 \cup \ldots \cup A_{N-1}$, the probability pr_i of visiting the interval A_i is determined for $0 \leq i \leq N-1$. If the statistical behavior of the map is influenced by the value of λ, then $pr_i = pr_i(\lambda)$ and the dependency of pr_i with respect to λ can be computed using some kind of statistical distance. In this Thesis the *Wootters' distance* is considered [Majtey05].

Definition 2.6.1 (Wootters' distance)**.** *Let us assume two probability distributions* $Pr_i = \left\{ pr_j^{(i)}, j = 1, \ldots, N \right\}$ *with* $i = 1, 2$*. The Wootters' statistical distance is given by*

$$\mathcal{D}_W(Pr_1, Pr_2) = \cos^{-1}\left(\sum_{j=1}^{N} \sqrt{pr_j^{(1)} \cdot pr_j^{(2)}} \right). \tag{2.66}$$

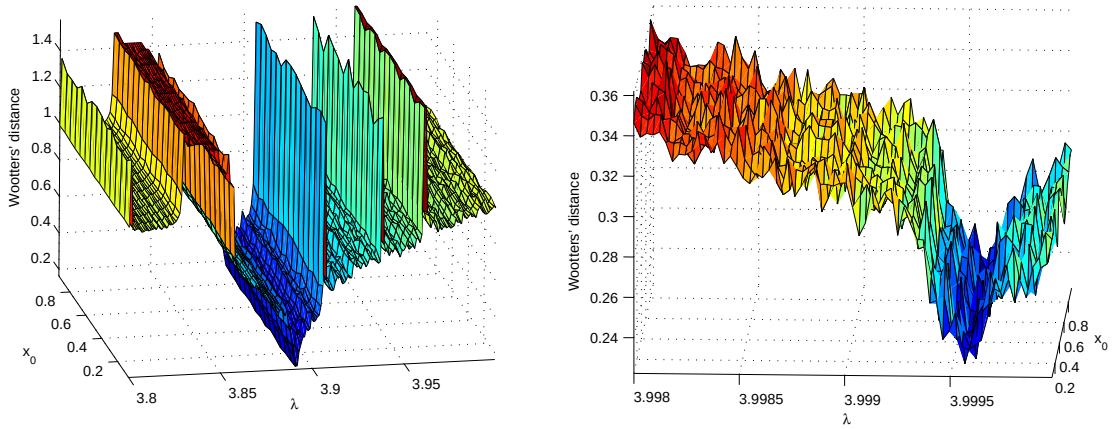
If $f_\lambda : \mathcal{U} \to \mathcal{U}$ is unimodal (see Definition 1.3.3) with $\mathcal{U} = [0, 1]$, then orbit of length M generated from $x_0 \in \mathcal{U}$ can be encoded into a binary sequence,

$$\mathbf{B}_M(f_\lambda, x_0) = \{B_i(f_\lambda, x_0)\}_{i=0}^{M-1} = \theta(f_\lambda^{(0)}(x_0))\theta(f_\lambda^1(x_0)) \ldots \theta(f_\lambda^{(M-1)}(x_0)), \tag{2.67}$$

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

$$\theta(y) = \begin{cases} 0, & \text{if } y < x_c \\ 1, & \text{if } y \geq x_c \end{cases} \tag{2.68}$$

A probability distribution can be obtained from $\mathbf{B}_M(f_\lambda, x_0)$ just by 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 $M - w + 1$ integers (or words), taking some of the 2^w possible values. 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 logistic 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. 2.20 for two values of $\hat{\lambda}$ with $M = 10^4$ and $w = 10$; the corresponding symbolic sequences were generated with different initial conditions. Figure 2.20 shows that around the right value of λ there exists a basin of attraction, which leads immediately to an estimation of $\hat{\lambda}$.



(a) $\hat{\lambda} = 3.890925$ (b) $\hat{\lambda} = 3.999567$

Figure 2.20: Wootter's distance of the logistic map with respect to the logistic map. The length of the symbolic sequences is $M = 10^4$, whereas the words are of width $w = 10$.

The Wootters' distance can also be used to discriminate between different probability distribution functions.

Case study 2.6.1 ([Arroyo09c]). *Cryptanalysis of the cryptosystem described in [Kurian08]*

As as example, let us consider the encryption system described in [Kurian08], whose structure is depicted in Fig. 2.21, and which has been cryptanalyzed by us [Arroyo09c]. In that encryption scheme the stochastic behavior of the symbolic se-

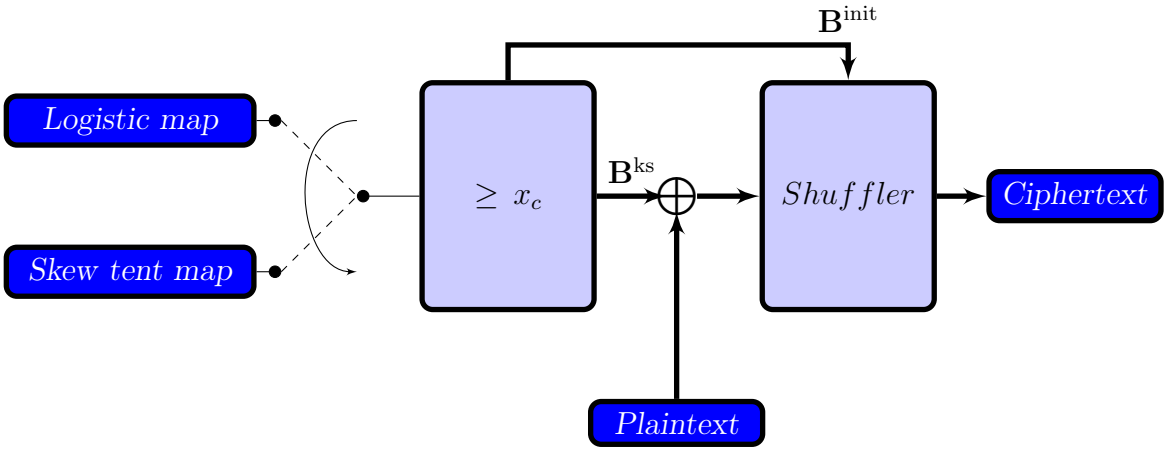


Figure 2.21: Stream cipher based on the binary sequences generated from the logistic map and skew tent map.

quences of the logistic map and skew tent map are used to build up a stream cipher. The plaintext is encrypted through the symbolic dynamics of either the logistic map or the tent map, with fixed control parameter λ and initial condition x_0. If the plaintext is M bit long, then $\gamma_{f_\lambda}^{M+Q}(x_0)$ is computed with the selected map according to Eq. (2.4), and Eq. (2.67) is used to produce a binary sequence. The scheme proposed in [Kurian08] divides the finite binary sequence

$$\mathbf{B}_{M+Q}(f_\lambda, x_0) = \{B_i(f_\lambda, x_0)\}_{k=0}^{M+Q-1} = \theta(f_\lambda^{(0)}(x))\theta(f_\lambda^{(1)}(x))\ldots\theta(f_\lambda^{(M+Q-1)}(x))$$

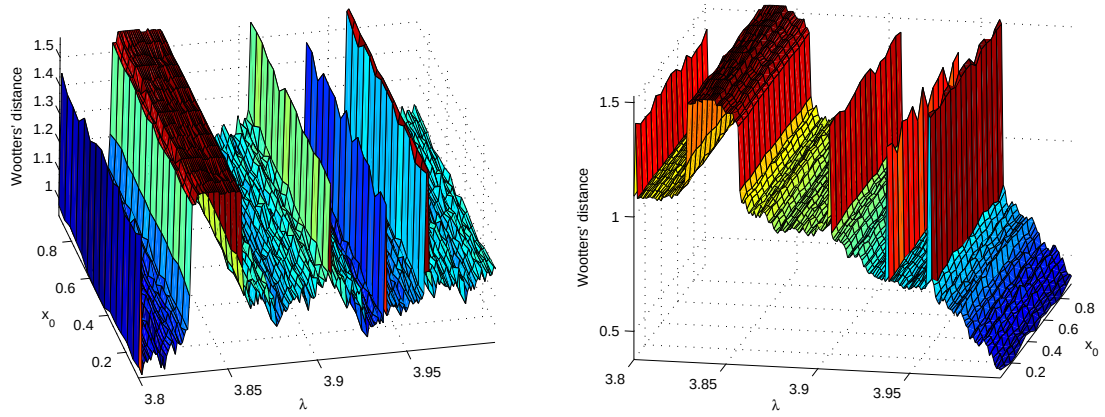
into two segments: $\mathbf{B}^{\text{init}} = \{B_i^{\text{init}}\}_{i=0}^{Q-1}$ with $B_i^{\text{init}} = B_i(f_\lambda, x_0)$, and $\mathbf{B}^{\text{ks}} = \{B_i^{\text{ks}}\}_{i=0}^{M-1}$ with $B_i^{\text{ks}} = B_{Q+i}(f_\lambda, x_0)$. The initial segment $\mathbf{B}^{\text{init}}$ encodes x_0 as it is done in [Stojanovski97]. The final segment $\mathbf{B}^{\text{ks}}$ is the *keystream* of the cipher, i.e., the plaintext $\mathbf{P} = \{P_i\}_{i=0}^{M-1}$ is transformed into the *pre-ciphertext* $\overline{\mathbf{C}} = \{\overline{C}_i\}_{i=0}^{M-1}$ according to

$$\overline{C}_i = P_i \oplus B_i^{\text{ks}} = P_i \oplus B_{Q+i}(f_\lambda, x_0), \tag{2.69}$$

where $i = 0, 1, \ldots, M-1$, and $0 \oplus 0 = 1 \oplus 1 = 0$, $0 \oplus 1 = 1 \oplus 0 = 1$. Finally, the pre-ciphertext $\overline{\mathbf{C}}$ and $\mathbf{B}^{\text{init}}$ are combined into the *ciphertext* or encrypted message $\mathbf{C} = \{C_i\}_{i=0}^{M+Q-1}$ which is sent to the receiver through an insecure channel. The

generation of $\mathbf{C}$ is driven by a shuffler block, implementing an injective map $\pi : \{0, 1, \cdots, Q-1\} \mapsto \{0, 1, \cdots, M-1, M\}$, which inserts the Q bits of $\mathbf{B}^{\text{init}}$ into the pre-ciphertext $\overline{\mathbf{C}}$.

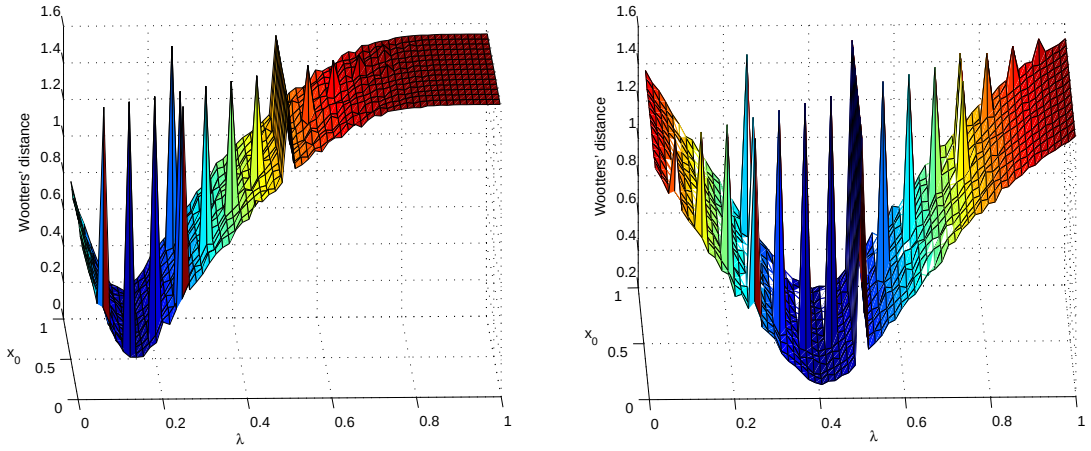
The secret key of the cryptosystem just defined includes the map to use in the generation of the keystream. In this sense, the authors of [Kurian08] assume that it is not possible to infer the map used in the generation of a given symbolic sequence. However, this is a wrong assumption, since the Wootters' distance can be used to identify the map employed in the generation of the keystream of the cryptosystem given in [Kurian08]. In a *chosen-plaintext attack*, a cryptanalyst has access to the encryption device and thus can obtain the output corresponding to any input. If $P_i = 0$ for $0 \leq i \leq M-1$, i.e., all the bits of the plaintext $\mathbf{P}$ are chosen to be zero, then $\overline{\mathbf{C}} = \mathbf{0} \oplus \mathbf{B}^{\text{ks}} = \mathbf{B}^{\text{ks}}$, and the corresponding ciphertext is $\mathbf{B}^{\text{shuffled}} = \pi\left(\mathbf{B}^{\text{init}} \| \mathbf{B}^{\text{ks}}\right)$, where $\|$ stands for "yuxtaposition". If we consider now that $\mathbf{B}^{\text{shuffled}}$ has been generated using the tent map with control parameter $\hat{\lambda}$, then Wootters' distance from $\mathbf{B}^{\text{shuffled}}$ to the logistic map produces a picture with no basin of attraction (see Fig. 2.22(a), where the Wootters' distance is always upper 0.9) or with a basin of attraction around $\lambda = 4$ (see Fig. 2.22(b)). In this case, we conclude that the chosen map is the logistic map



(a) $\hat{\lambda} = 0.138891$ (b) $\hat{\lambda} = 0.409249$

Figure 2.22: Wootter's distance of the skew tent map with respect to the logistic map.

with $\hat{\lambda} = 4$, or the tent map with an unknown value for the control parameter. A further analysis of Wootters' distance to the tent map makes possible to discard the logistic map in this situation. Figure 2.23 depicts Wootters' distance to the tent map when $\mathbf{B}^{\text{shuffled}}$ is generated using the tent map with two different values for $\hat{\lambda}$. Again, it is possible to discern a basin of attraction around $\hat{\lambda}$, which has been verified for different random configurations of the interleaving of $\mathbf{B}^{\text{init}}$ and $\mathbf{B}^{\text{ks}}$.



(a) $\hat{\lambda} = 0.138891$ (b) $\hat{\lambda} = 0.409249$

Figure 2.23: Wootter's distance of the skew tent map with respect to the skew tent map for $N = 10^4$ and $w = 10$.

2.7 Analysis of the dense periodic points of chaos

Chaos is the result of the paradoxical association between a local divergence and a global convergence. As a result of this peculiar relationship, the wandering behavior of chaos is sustained by a set of dense *Unstable Periodic Orbits* or *UPOs*. Furthermore, the thorough knowledge of the distribution of the UPOs of a chaotic system allows the reconstruction of its dynamics [Cvitanović91]. In other words, UPOs can be interpreted as the *skeleton* of chaos. In this sense, the level of randomness of chaos is a consequence of the complexity of the distribution of UPOs, which could imply that a high value of entropy entails a large set of UPOs. Therefore, the randomness of chaos could leak the underlying regularity, which results in a reduction of the *complexity* of the behavior of the chaotic system. Consequently, mathematical tools to analyze the complexity of a chaotic system should be defined. Maximum complexity is achieved only for a pure random process, i.e., a process with maximum entropy and which does not contain any structural correlation. In other words, maximum complexity is assure only for a uniform probability distribution function. As a result, the degree of complexity of a given probability distribution can be calculated through its *statistical divergence* from the uniform probability distribution. A very useful measure of statistical divergence is the one defined by Jensen [Martin06].

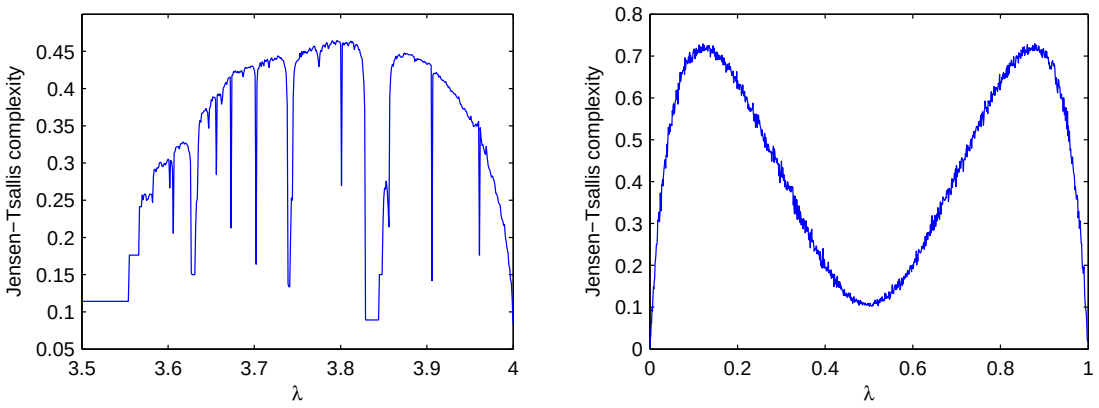
Definition 2.7.1 (Jensen's divergence)**.** *Consider two discrete distributions* $Pr_i = \left\{pr_1^{(i)}, \ldots, pr_N^{(i)}\right\}$*, for* $i = 1, 2$*. Let* H *be a functional entropic form of both probability*

distributions. The associated Jensen's divergence is defined by

$$J_H^{\beta}\left(Pr_1, Pr_2\right) = H\left(\beta Pr_1 + (1-\beta)Pr_2\right) - \beta H\left(Pr_1\right) - (1-\beta)H\left(Pr_2\right), \qquad (2.70)$$

where $0 \leq \beta \leq 1$.

If $\beta = 1/2$ and $pr_j^{(2)} = 1/N$ for $j = 1, \ldots, N$, then the Jensen's divergence is a measure of the statistical complexity of the probability distribution Pr_1. The structural complexity of chaos lies on the underlying UPOs. If the distribution of UPOs changes as the control parameters do, then the statistical complexity could bring to light a hint to infer the values of the control parameters. For instance, let us consider the case of the logistic map and skew tent map. For both maps the statistical complexity was determined using the Tsallis' entropy with $q = 0.9$ (Eq. (2.27)). In Fig. 2.24(a) appears the Jensen-Tsallis statistical complexity of the logistic map versus the control parameter. It shows that the statistical complexity is very related to the value of the control parameter in the chaotic region. In fact, the complexity is almost a bijective function of the control parameter in the chaotic region, and thus it could be used to estimate the value of the control parameter. On the other hand, the statistical complexity of the skew tent map is a two-to-one



(a) (b)

Figure 2.24: Statistical complexity Jensen-Tsallis of (a) the logistic; (b) and the skew tent map for different values of λ and $q = 0.9$.

function of the control parameter. The skew tent map has an uniform probability distribution function, which could make us to consider it as a total random process. Nevertheless, we must not forget that the apparently disorder of chaos is sustained by an underlying regularity. In the case of the skew tent map this regularity can be extracted by analyzing its associated symbolic sequences. Indeed, the skew tent

map has a Lebesgue measure on $[0, 1]$, which is an ergodic invariant measure of the tent map for all $\lambda \in (0, 1)$. In [Li05b] it is shown that the invariant measure of the skew tent map implies that the ratio between the number of 1-bits and 0-bits in a typical orbit coincides with the ratio between the lengths of the intervals $[\lambda, 1]$ and $[0, \lambda)$, namely, $\frac{1-\lambda}{\lambda}$. For the sake of illustration, the control parameter of the skew

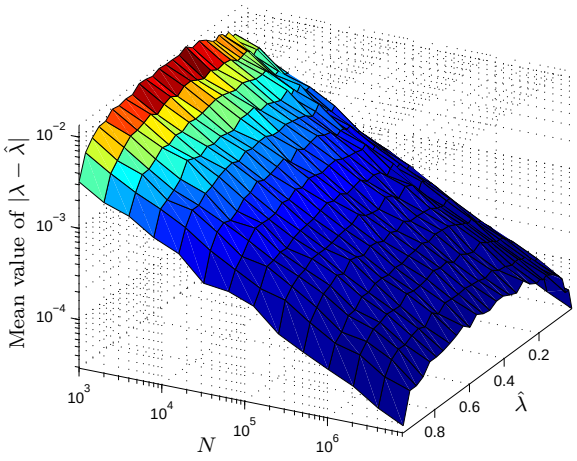


Figure 2.25: Error in the estimation of the control parameter of the tent map from the ratio between 1-bits and 0-bits in a given symbolic sequence.

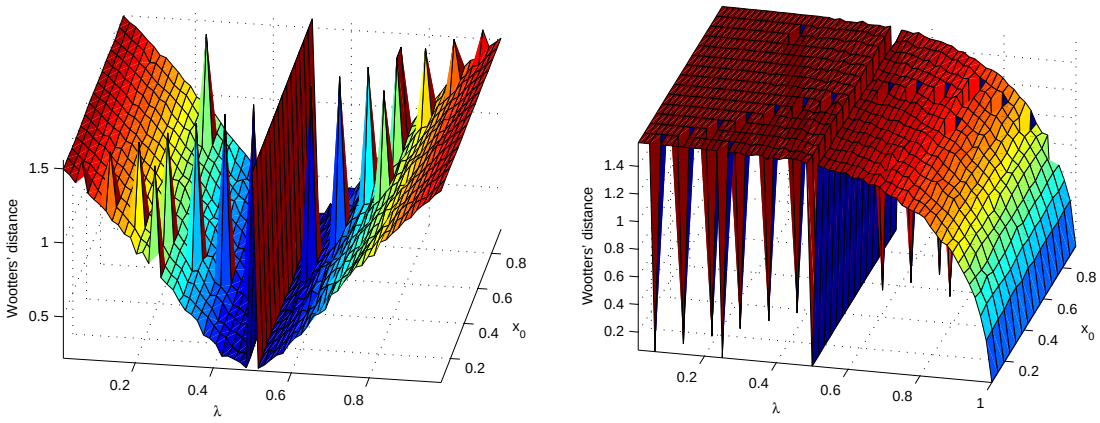
tent map was estimated from the ratio 0-bits and 1-bits of the symbolic sequences generated for different values of the control parameter and the initial condition (see Fig. 2.25). As it is expected, the larger the symbolic sequences, the smaller the error in the estimation.

The approximation of the underlying regularity of chaos is the base of many techniques used in the analysis of chaotic time series. As matter of fact, the reconstruction of the dynamics of a chaotic system from the associated time series is well known from the milestone work of Takens [Takens81]. Taken's theorem is the base of a great variety of methods used in the analysis of time series [Farmer87; Tsonis07; Letellier08], but it is also possible to perform that analysis using techniques based on different theoretical backgrounds, as the analysis of recurrence plots [Marwan07], the wavelet transform [Cao95; Billings05; Masuda01] or neural networks [Bakker00; Al-Assaf04; Gholipour06]. Specially interesting are the methodologies based on symbolic dynamics [Wu04; Piccardi06; Buhl07; Wang08a] and analysis of *order patterns* [Bandt05; Amigó06; Bandt07]. Certainly, for some chaotic systems those tools are a very useful help in the discovering of bijective or quasi-bijective functions that guide the estimation of the control parameter and, maybe, the initial

condition associated to a chaotic orbit. Unimodal maps are an example of chaotic systems allowing that estimation. In the following two Chapters it is studied the symbolic dynamics of unimodal maps, and second the distribution of their order patterns. The goal of both Chapters is to illustrate how to use either symbolic dynamics or order patterns to estimate the control parameters of a chaotic map.

2.8 Digital degradation

A major problem when dealing with chaotic maps is their implementation. If the chaotic maps are implemented digitally, then a degradation of their dynamics is induced by finite precision arithmetics. Certainly, for a precision of N bits, the number of possible states is 2^N and thus the iteration of a chaotic system will eventually be periodic. For that reason, the orbits generated by iteration of the digital implementation of a chaotic map are called *pseudo orbits* instead of chaotic orbits. According to the *Anosov's shadowing theorem* [Brin03, p. 113], there always exists an exact chaotic orbit close to a given pseudo orbit with only an small error. Nevertheless, Anosov's theorem is useless for digital chaos, since the shadowing orbits are generally of measure zero. As a result, the digital implementation of chaos could imply a loss of ergodicity, a deviation from the theoretical invariant measure, or a positive Lyapunov exponent. An extreme example of digital degradation is the skew tent map. As it has been pinpointed in Sec. 2.7, the ergodicity of the skew tent map allows to estimate the control parameter just analyzing the rate between 0-bits and 1-bits in its symbolic sequences. It was emphasized that the precision in the estimation can be improved by increasing the length of the symbolic sequences. However, that precision is bounded in a practical context as a result of the deviation of the invariant measure from its theoretical value. Another proof of the dynamical degradation of the skew tent map can be found using the Wootters' distance. Indeed, the peaks appearing in Fig. 2.22 are a consequence of low period orbits for some values of the control parameter and the initial condition of the *digital* skew tent map. Moreover, digital degradation also destroys the *topological conjugacy* between the logistic map and symmetric tent map (the skew tent map with $\lambda = 1/2$) [Hao98, p. 68]. According to the topological conjugacy, the Wootters' distance of the logistic map with $\lambda = 4$ to the skew tent map should be identical to the Wootters' distance of the symmetric tent to the skew tent map. However, Fig. 2.26 spells out a clear difference between them, since digital degradation causes "peaks" for the logistic map but "shafts" for the symmetric tent map. As a result, from a practical point of view it is possible to discern between both maps even when there exists topological conjugacy, since when working with finite



(a) (b)

Figure 2.26: Wootters' distance of the (a) logistic map for $\hat{\lambda} = 4$ and $x_0 = 0.593563$; and (b) the skew tent map for $\hat{\lambda} = 1/2$ and $x_0 = 0.213988$ respect to the skew tent map for $N = 10^4$ and $w = 10$. The quantization steps of x- and y-axis are 2^{-6} and 2^{-4} respectively.

precision arithmetics the symmetric tent map possesses a "digitally stable" [1] fixed point at $x = 0$. As a result, the main conclusion of this section is that the use of a chaotic map in the context of chaos-based cryptography requires a full and thorough analysis of all its dynamical properties. It has to be determined the effect of digital degradation as it is done in [Li03, Chapter 3].

2.9 Concluding remarks

In this Chapter we have shown that, although chaotic systems possess a behavior very useful for the design of encryption procedures, we cannot assume that a chaotic system fulfills the needs of cryptography just because it evolves chaotically. Indeed, it is necessary to test and verify that the properties of the dynamical systems used as based of cryptosystems do really meet the standard requirements of cryptography. With this regard, we have defined a set of mathematical indicators to guide the assessment of the adequacy of orbits of dynamical systems for cryptographical applications. The Lyapunov exponent is the figure to conclude the potentiality of orbits as sources of *diffusion* of information, whereas different measures of entropy

[1] The term "digitally stable" means that the fixed point is stable under finite computing precision. That is, any chaotic orbit will finally lead to $x = 0$ after a limited number of iterations. The number of iterations has an upper bound determined by the finite precision. Some discussions on this phenomenon with floating-point arithmetic can be found in [Li04a].

have been introduced in order to evaluate the performance of orbits as generators of *confusion* of information. Since in the context of chaos-based cryptography confusion is done by embedding the information into the chaotic orbits in different ways, the entropy should be analyzed from many points of view as possible. Therefore, entropy must be calculated not only through the partition of the state space, but also by the analysis of energy in the frequency domain. However, confusion property does not only lie on the level of entropy of orbits. Certainly, it is also required orbits with a probability distribution non-depending on the control parameters, and thus the histograms of orbits must be calculated and analyzed using measures of statistical distance to confirm this need. Finally, the fulfillment of confusion property also requires that mathematical indicators extracted from chaotic orbits do not allow the estimation of either the control parameters, or the initial condition, or both. In this sense, we must establish if and how the orbits can be transformed to later compute a mathematical indicator revealing a one-to-one or few-to-one relation to the control parameters and/or the initial condition. This assessment allows a series of context where the orbits leaks the parameters controlling their dynamics. This is crucial for the design of secure chaos-based cryptosystems. Indeed, the design of a chaos-based cryptosystem must define the use of chaotic orbits taking into account those critical contexts. More precisely, it must guarantee the impossibility of reproducing any of those contexts in any of the situations defined by the four cryptanalysis scenarios defined in Sec. 1.2.2. The consequences of a neglected design have been shown in this Chapter through a series of cryptanalysis works of our own. In the next Chapter we show that the theory of symbolic dynamics also reveals another critical context and, consequently, it should be handled during the design of a chaos-based cryptosystem.

Chapter 3

Symbolic dynamics of unimodal maps

3.1 Introduction

In the spirit of the previous Chapter, we continue on the characterization of chaotic maps focusing now the attention on "coarse-grained" versions of their orbits. Recalling Chaos Theory, the first step when studying some special type of complex temporal evolution (i.e., chaotic temporal evolution) was simplification by means of mathematical concretion. A complementary strategy is based on the partition of the phase space of chaotic maps. As a matter of fact, chaotic maps are continuous-state discrete-time systems that can be converted into discrete-state discrete-time systems, which implies that the further study is done on sequences of symbols or *symbolic sequences* instead of sequences of real numbers. The result of such transformation defines an special area in the Theory of Dynamical Systems which is *symbolic dynamics*. As it is pointed out in [Kitchens97, p. V], Jacques Hadamard was the first to use infinite sequence of symbols to analyze dynamics. In 1930's and 40's symbolic dynamics were the basis of the work of Hedlund and Morse, and also of Shannon's description of information channels. Later, symbolic dynamics has been broadly used in the study of dynamical systems [Metropolis73; Hansen92; Hao98; Pastor06; Pastor07a; Pastor07b; Pastor07c; Pastor07d; Pastor08; Pastor09; Romera08; Wang08a] , Markov shifts [Lind95; Kitchens97], time-series [Daw03], and also in the cryptanalysis of chaos-based cryptosystems [Wang05; Alvarez07a; Alvarez07b; Arroyo09f].

A crucial step in symbolic dynamics is to partition the phase space conveniently. The criterion in this regarding is based on the analysis of entropy, as it was explained in Sec. 2.4. In Definition 2.4.1 it was defined the concept of generating partition, i.e., the partition adequate to lead the discretization of orbits. The existence of a generating partition is guaranteed for any ergodic chaotic system [Krieger70], but its determination is generally very difficult (different methods can be found in [Steuer01;

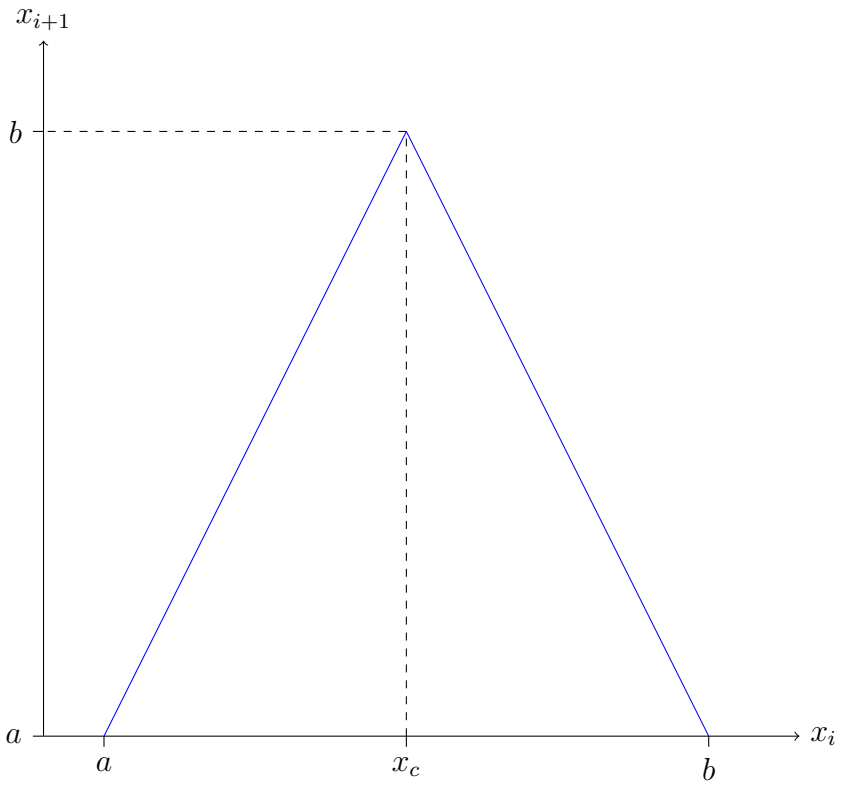


Figure 3.1: Skew tent map for $\lambda = 1/2$ also known as symmetric tent map.

Kennel03; Buhl05; Rajagopalan06]). Nevertheless, in the context under consideration, generating partitions are obtained directly. Certainly, for the class of maps in $\mathcal{F}$ a generating partition is given by $\{[0, x_c), [x_c, 1]\}$, which determines the transformation of orbits into sequences of two symbols.

A symbolic sequence for an unimodal map is a transformation of a sequence of real numbers into a sequence consisting of a pair of symbols. These two symbols represent the relative position of a real-value iterate with respect to the critical point of the underlying iteration function of a unimodal discrete-time chaotic system. The existence of an inner order of the symbolic sequences of maps in $\mathcal{F}$ and the relationship between this order and the initial condition and the control parameter of the underlying chaotic system are pointed out in [Metropolis73]. The considerations and results of [Metropolis73] were later improved and enlarged through different contributions, being the most important [Beyer86] and [Wang87]. In [Alvarez98] it was remarked that the order of the symbolic sequences can be interpreted using the concept of *Gray codes*. In this novel approach to the problem, the symbolic sequences are finally converted into a figure which is a real number between 0 and 1 called *Gray Ordering Number* or simply *GON*. Afterwards, [Cusick99] drew the bridge between

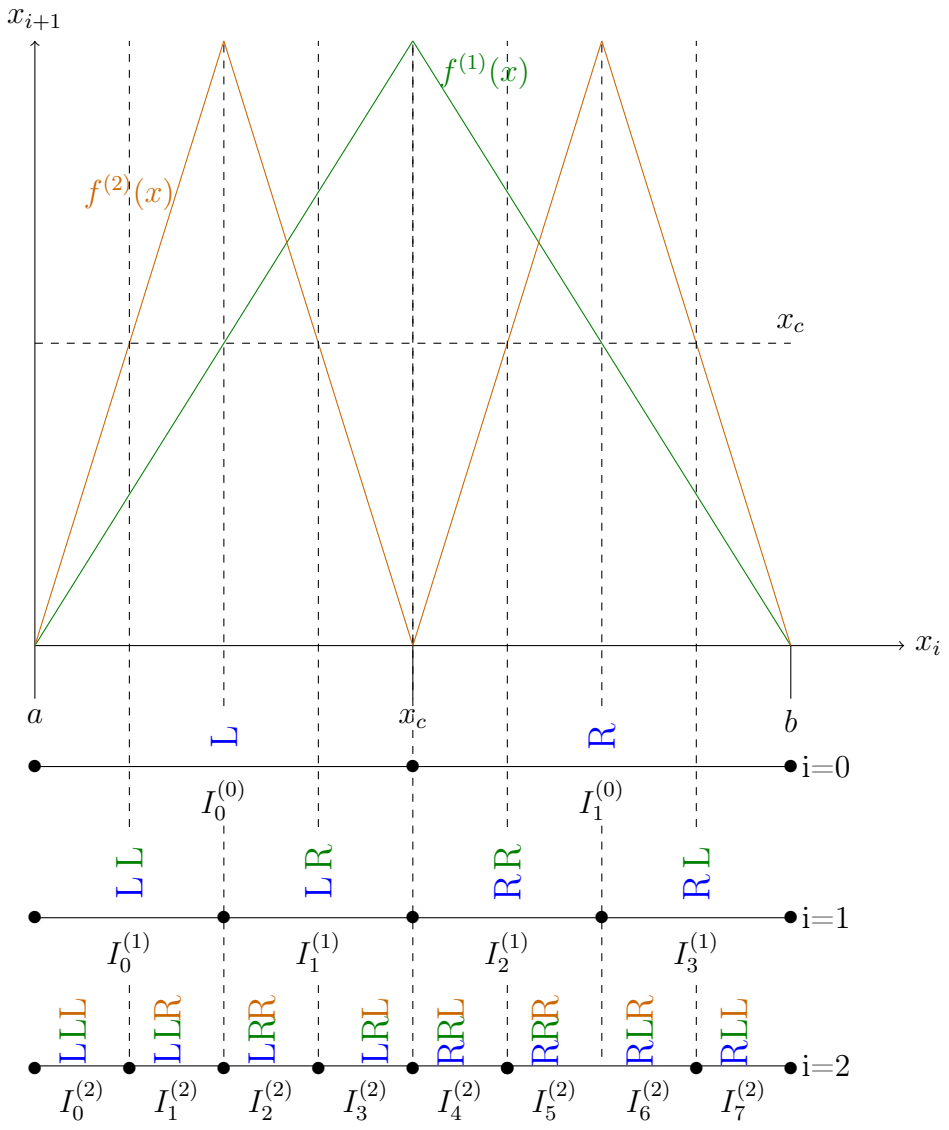


Figure 3.2: Symbolic intervals for different iterations of the tent map.

the ideas of [Alvarez98] and the main theory of applied symbolic dynamics as expressed in [Wang87]. Finally, some theorems are suggested in [Wu04], which enlarge the theoretical framework of the GON of unimodal maps. In [Wu04] it is explained that the dynamical properties of unimodal maps by means of the GON are a translation of the theoretical framework inherited from [Metropolis73]. Nevertheless, there is no direct and explicit proof of this equivalence. Since the main application of the concept of the GON is the estimation of the control parameter of unimodal maps for cryptanalysis [Alvarez03b], a rigorous and concrete theoretical framework is required. This Chapter presents this concretion and also shows that some of the theorems in [Wu04] are not totally accurate. In this sense, those theorems are not only criticized

but also rewritten.

The rest of the Chapter is organized as follows. Section 3.2 remarks the existence of an inner order for the symbolic sequences of a certain class of unimodal maps and a relationship between that order and the order of the initial conditions employed in their generation. In Sec. 3.3 the order of the symbolic sequences is rewritten in terms of Gray codes and the concept of Gray Ordering Number is introduced. After that, Sec. 3.4 introduces a subclass of the class of considered unimodal maps. This subclass of unimodal maps is defined in a parametric way, i.e., their dynamics depend on a control parameter. This dependency is analyzed by means of the GON. This study will lead to the revision and proof of all theorems in [Wu04]. In Sec. 3.5 the previous theoretical framework is applied to the estimation of the initial condition and the control parameter of unimodal maps, which is linked between symbolic dynamics and cryptanalysis of chaos-based cryptosystems. The main consequences of the theoretical work and its application are recapitulated in Sec. 3.6.

3.2 Relationship between the symbolic sequences and the initial condition used in their generation

Let us consider the case of the *symmetric tent map* (i.e., the skew tent map for $\lambda = 1/2$) shown in Fig. 3.1. The symmetric tent map satisfies Definition 1.3.3, which implies that a certain value $x_{i+1} \neq x_c$ can be derived from two different values of x_i, as Fig. 3.1 informs. In other words, it is satisfied that $x_{i+1} = f(x_i^L) = f(x_i^R)$, where $x_i^L \neq x_i^R$, $x_i^L < x_c$ and $x_i^R > x_c$. This is a common characteristic of all the functions of the class $\mathcal{F}$. It means that the initial condition used in the generation of $\{x_i\}$ using $f(x) \in \mathcal{F}$ can be recovered from the last number of the sequence only if the relative position of every x_i with respect to x_c is known. Therefore, the recovering of the initial condition demands recording those relative positions. This is achieved by transforming $\{x_i\}$ into a symbolic sequence or pattern according to the next criterium:

$$x_i \equiv L \text{ if } x_i \in [a, x_c), \tag{3.1}$$

$$x_i \equiv C \text{ if } x_i = x_c, \tag{3.2}$$

$$x_i \equiv R \text{ if } x_i \in (x_c, b]. \tag{3.3}$$

Consequently, $\{x_i\}$ is associated to the symbolic sequence $S = s_0 s_1 \ldots$ where $s_i \in \{L, R\}$. Using S and the last element of $\{x_i\}$ one can recover the initial condition x_0.

Let us call $S_f(x_0)$ to the symbolic sequence of length M generated from x_0 using the function $f(x)$, which is included in the class $\mathcal{F}$. The value of the $i-$th symbol

of the symbolic sequence $S_f(x_0)$ is determined by $f^{(i)}(x_0)$, i.e., the $i-$th iteration of $f(x)$ from x_0 for $i \in [0, M-1]$. If S_i is the $i-$th symbol of the symbolic sequence, S_i is equal to L if and only if $f^{(i)}(x_0) < x_c$. In the same way, p_i is equal to R if and only if $f^{(i)}(x_0) > x_c$. As a consequence, the definition interval $\mathcal{U}$ is divided into 2^{i+1} *symbolic* subintervals. Indeed, if $x_c^{(i,j)}$ is the j-th solution of the equation

$$f^{(i)}(x) = x_c, \tag{3.4}$$

the set $\left\{x_c^{(i,j)}\right\}$ for $0 \leq j < 2^i$ divide the definition interval into 2^{i+1} subintervals, where $x_c^{(0,0)} = x_c$. All the values included in one of these intervals generate the same symbolic sequence of length $i+1$. In Fig. 3.2 the symbolic intervals of the tent map for zero, one and two iterations are depicted. The main result of the previous proposition is that, for a certain number of iterations, the different subintervals are so that two neighboring subintervals lead to the same symbolic sequence except for one symbol. On the other hand, for $i \in \mathbb{N} \cup \{0\}$ and $j \in [0, 2^i - 1]$, the set of points $x_c^{(i,j)}$ determine periodic symbolic sequences of period $i+1$ when they are considered as initial conditions. If the symbol C is assigned to x_c and only one period is regarded, the symbolic sequences generated from $\left\{x_c^{(i,j)}\right\}$ end with a C. In this sense, if the iteration process associated to the generation of a symbolic sequence stops just when a C is obtained, only the symbolic sequences derived from the set of initial conditions solution of Eq. (3.4) have finite length.

If $\mathcal{S}$ is the set of all sequences derived from the iteration of the functions included in $\mathcal{F}$, then it is possible to derive a complete ordered set $(\mathcal{S}, <_{\mathcal{S}})$ where the referred order is defined according to [Beyer86, p. 309] as follows:

Lema 3.2.1 ([Beyer86]). *Assuming $L <_{\mathcal{S}} C <_{\mathcal{S}} R$, $S = \{s_i\}$ and $T = \{t_i\} \in \mathcal{S}$, and j is the first index so that $s_j \neq t_j$, it is said that $S <_{\mathcal{S}} T$ if one of the next conditions is satisfied:*

1. *$j = 0$ and $s_0 <_{\mathcal{S}} t_0$.*
2. *$j > 0$, $s_0 s_1 \ldots s_{j-1} = t_0 t_1 \ldots t_{j-1}$ contains an even number of R's and $s_j <_{\mathcal{S}} t_j$.*
3. *$j > 0$, $s_0 s_1 \ldots s_{j-1} = t_0 t_1 \ldots t_{j-1}$ contains an odd number of R's and $s_j >_{\mathcal{S}} t_j$.*

The inner order of $\mathcal{S}$ is directly linked to the order on $\mathbb{R}$ of the real numbers in $\mathcal{U}$ used to generate the symbolic sequences from any f in $\mathcal{F}$. This is informed and proved in [Beyer86, Lemma 4.1] and in [Wang87, Theorem 2]. For the sake of clarity, the relationship between the order of the kneading sequences and the order of the initial conditions is rewritten as a theorem:

Theorem 3.2.1 ([Beyer86; Wang87]). *For $f(x)$ belonging to the class of functions $\mathcal{F}$ and x, y included in the interval of definition of $f(x)$ so that $x < y$, it is verified that $S_f(x) \leq_{\mathcal{S}} S_f(y)$.*

3.3 Gray codes and symbolic sequences

In the previous section it was remarked that $f^{(i)}(x)$ can be divided into 2^{i+1} intervals such that all the values included in one of those intervals lead to the same symbolic sequence of length $i+1$. In this sense, those intervals were referred as symbolic intervals, since a certain interval can be named through the symbolic sequence generated from any value inside it. It was also observed that two contiguous symbolic sequences differed in just one symbol. Finally, if the first symbol of the symbolic sequences is discarded, the 2^{i+1} symbolic subintervals generated by the $i-$th iteration of the map $f(x)$ are symmetric with respect to $x = x_c$. In communication theory it is very well known a family of codes distinguished by the fact that two successive codes only differ in one bit. This family of codes is the Gray codes family, which also presents the above cited mirroring property. Table 3.1 shows the Gray codes of length 4. As a result, it is immediate the translation of the symbolic sequences of the class of functions $\mathcal{F}$ into binary sequences just changing the symbol L into 0 and the symbols R and C into 1 [Alvarez98]. In this sense, the Gray code associated to a certain pattern $S_f(x)$ is given by the next definition.

Definition 3.3.1. *The Gray code corresponding to $S_f(x) = s_0 s_1 \cdots s_{i-1} \cdots$ is defined as $G(S_f(x)) = g_0 g_1 \cdots g_{i-1} \cdots$ where*

$$g_i = \begin{cases} 1, & \text{if } s_i = R \\ 0, & \text{if } s_i = L \end{cases}$$

for $i \in \mathbb{N} \cup \{0\}$. If $s_j = C$ for any j in $\mathbb{N} \cup \{0\}$, then the Gray code associated to $S_f(x)$ is $g_0 g_1 \cdots g_{j-1}$.

As Table 3.1 informs, it is possible to translate a Gray code into a binary code. The equivalent binary code of a given Gray code can be easily obtained using the next definition:

Definition 3.3.2. *If the Gray code of a symbolic sequence $S_f(x) = s_0 s_1 \cdots s_{i-1} \cdots$ is given by $G(S_f(x)) = g_0 g_1 \cdots g_{i-1} \cdots$, then the binary code related to $S_f(x)$ is $U(S_f(x)) = u_0 u_1 \cdots u_i \cdots$ where*

$$u_i = u_{i-1} \oplus g_i,$$

for $i \in \mathbb{N}$ and $u_0 = g_0$. If $S_f(x)$ is of length j, i.e., if $S_j = C$, then the binary code related to $S_f(x)$ is $U(S_f(x)) = u_0 u_1 \cdots u_j$ where $u_0 = g_0$, and

$$u_i = \begin{cases} u_{i-1} \oplus g_i, & \text{for } 0 < i \leq j-1 \\ 1, & \text{for } i = j \end{cases}$$

Since a binary code can be interpreted as a decimal number just changing the base, it is possible to associate a number to a symbolic sequence. However, the canonical base changing makes the first symbol modify its weight as the length of the symbolic sequence increases. In order to avoid the changing of the symbol weights as the length of the symbolic sequences increases, the Gray code associated to a symbolic sequence is interpreted as a decimal number with integer part equal to zero. The next definition introduces how to carry out the transformation of a symbolic sequence into a real number between 0 and 1.

Table 3.1: Correspondence between Gray codes and binary codes for four bits.

Rank	**Binary code**	**Gray code**
0	0000	0000
1	0001	0001
2	0010	0011
3	0011	0010
4	0100	0110
5	0101	0111
6	0110	0101
7	0111	0100
8	1000	1100
9	1001	1101
10	1010	1111
11	1011	1110
12	1100	1010
13	1101	1011
14	1110	1001
15	1111	1000

Definition 3.3.3. *Let $G(S) = g_0 g_1 \cdots g_{M-1}$ be a set of bits representing a Gray code of length M. Let $U(S) = u_0 u_1 \cdots u_{M-1}$ be the binary code corresponding to $G(S)$. The **Gray Ordering Number** or **GON** of S is defined as the real number given by*

$$GON(S) = 2^{-1} \cdot u_0 + 2^{-2} \cdot u_1 + \cdots + 2^{-M} \cdot u_{M-1}.$$

The definition of the GON also implies the definition of an order $<_{GON}$ upon the set of symbolic sequences $\mathcal{S}$. In other words, according to the definition of the

GON, it is possible to build the complete ordered set $(\mathcal{S}, <_{GON})$. This ordered set is equivalent to $(\mathcal{S}, <_{\mathcal{S}})$, i.e., the order defined using the GON is equivalent to the order $<_{\mathcal{S}}$.

Proposition 3.3.1. *The orders $<_{\mathcal{S}}$ and $<_{GON}$ are equivalent on $\mathcal{S}$.*

Proof. Let $S = s_0 s_1 \dots s_{j-1} s_j \dots$ be a certain symbolic sequence which can be of finite or infinite length. If $U(S) = u_0 u_1 \dots u_{j-1} u_j \dots$ is the binary code linked to the kneading sequence S, u_j is equal to 1 if one of the next situations occurs:

1. $s_j = R$ and $s_0 s_1 \dots s_{j-1}$ contains an even number of R's.
2. $s_j = L$ and $s_0 s_1 \dots s_{j-1}$ contains an odd number of R's.

Let $Q = q_0 q_1 \dots q_{k-1} q_k \dots$ be another kneading sequence of finite or infinite length. Let $U(Q) = t_0 t_1 \dots t_{k-1} t_k \dots$ be its associated binary code. According to Theorem 3.2.1, if the first different symbol between S and Q is the $i-$th one, then $S <_{\mathcal{S}} Q$ if and only if one of the next cases happens:

1. $s_i = R$, $q_i = L$ and $s_0 s_1 \dots s_{i-1}$ contains an odd number of R's. As a consequence, it is verified that $u_i = 0$ and $t_i = 1$, which implies that $GON(S) < GON(Q)$, i.e., $S <_{GON} Q$.
2. $s_i = R$, Q of length i and $s_0 s_1 \dots s_{i-1}$ contains an odd number of R's. Since Q is of finite length, its final symbol is C. Therefore, $t_i = 1$ and $u_i = 0$ implying that $GON(S) < GON(Q)$, i.e., $S <_{GON} Q$.
3. $s_i = L$, $q_i = R$ and $s_0 s_1 \dots s_{i-1}$ contains an even number of R's. For this configuration, $u_i = 0$ and $t_i = 1$, which informs $GON(S) < GON(Q)$ and subsequently $S <_{GON} Q$.
4. S of length i, $q_{i-1} = R$ and $s_0 s_1 \dots s_{i-2}$ contains an even number of R's. Since S has i symbols, it means $u_{i-1} = 1$. On the other hand, $t_{i-1} = 1$ and three possible situations are
   (a) Q is of length j for $j > i$. Then $t_{j-1} = 1$ implies $GON(S) < GON(Q$.
   (b) Q is infinite-length and $q_i = L$, implying $t_i = 1$ and $GON(S) < GON(Q)$.
   (c) Q is infinite-length and $q_i = R$. In this case there exists $j > i$ such that $q_j = R$. Otherwise, the condition $S <_{\mathcal{S}} Q$ implies that S is of length 1 and $Q = RLLLL \dots$. In each of these situations it is satisfied $GON(S) < GON(Q)$.

On the other hand, let us assume $S <_{GON} Q$ and i the first index such that $u_i \neq t_i$.

1. $u_i = 0$, $t_i = 1$ and $s_0 s_1 \dots s_{i-1}$ contains an odd number of R's. Since $GON(S) < GON(Q)$, then $p_i = R$ and $q_i = L$, which further implies that $S <_{\mathcal{S}} Q$.

2. $u_i = 0$, $t_i = 1$ and $s_0 s_1 \dots s_{i-1}$ contains an even number of R's. In this situation the assumption $GON(S) < GON(Q)$ forces $s_i = L$ and $q_i = R$, which informs that $S <_{\mathcal{S}} Q$.

3. S is of length i, $t_{i-1} = 1$. This implies that $s_0 s_1 \dots s_{i-2}$ contains an even number of R's, $q_{i-1} = R$ and thus $S <_{\mathcal{S}} Q$.

4. $u_{i-1} = 0$ and Q of length i and $s_0 s_1 \dots s_{i-1}$ contains an odd number of R's. Therefore, $s_{i-1} = R$, $q_{i-1} = C$ and $S <_{\mathcal{S}} Q$.

As a result, $S <_{\mathcal{S}} Q$ if and only if $S <_{GON} Q$ and the proof is complete. □

The previous proposition and Theorem 3.2.1 lead to the next theorem, which represents the extension of Theorem 1 in [Wu04].

Theorem 3.3.1 ([Wu04]). *For $f \in \mathcal{F}$ and $x, y \in \mathcal{U}$, it is satisfied that $GON(S_f(x)) \leq GON(S_f(y))$ if and only if $x \leq y$. In other words, the GON of the symbolic sequences in $\mathcal{S}$ is an increasing function with respect to the initial condition.*

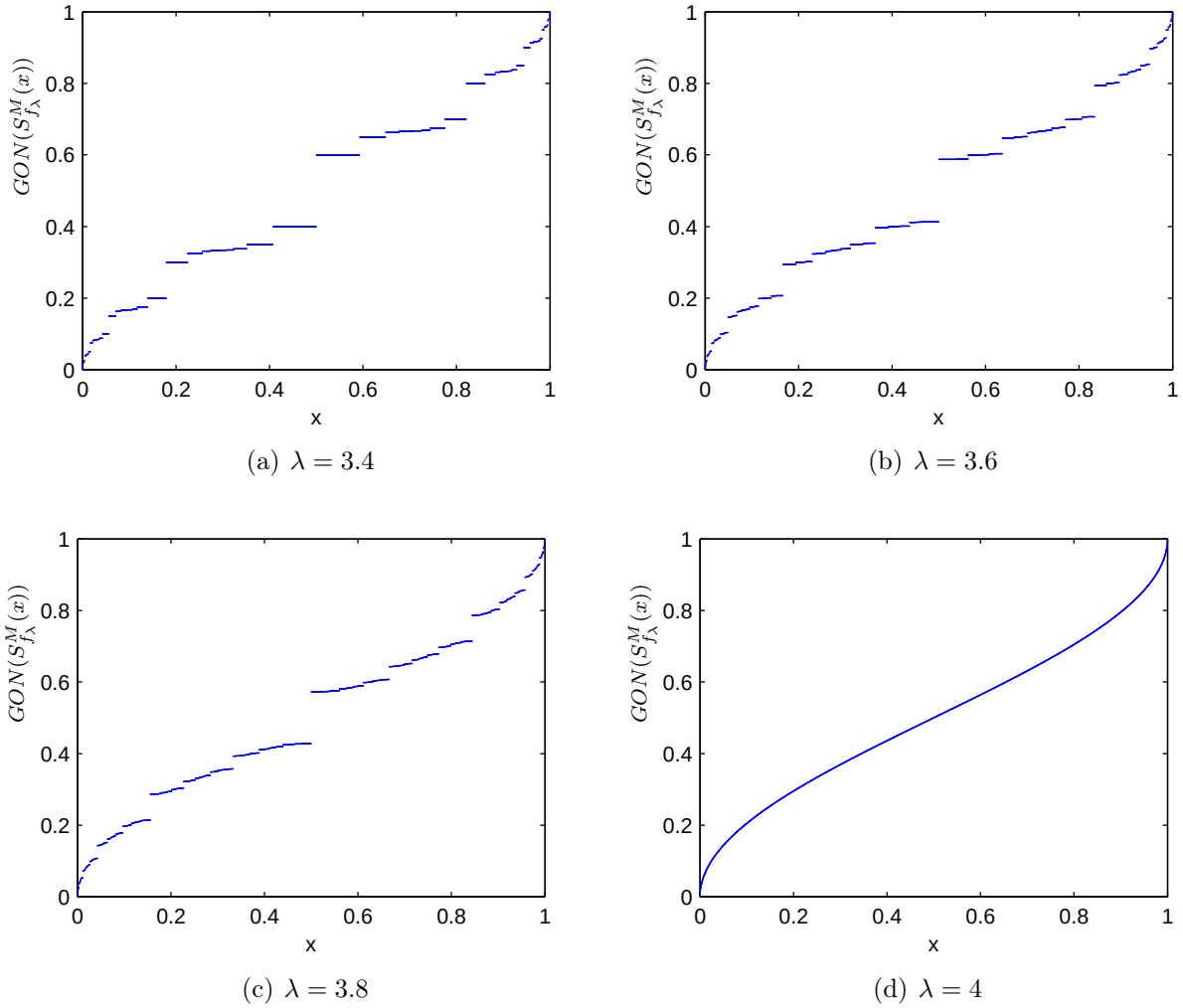
According to this theorem, the GON is an increasing function with respect to the initial condition, as it is shown in Fig 3.3 for the logistic map. That figure has been calculated working with symbolic sequences obtained by iterating M times the logistic map. Hereafter those symbolic sequences are denoted as $S^M_{f_\lambda}(x)$. The symbolic sequences given by $S^M_{f_\lambda}(x)$ are implicitly ended by C, all of them are of length M, and dependent on the iteration of a map defined in a parametric way.

3.4 Gray codes and parametric unimodal maps

A special case of interest is the study of unimodal maps defined in a parametric way. In this sense, this section is focused on the analysis of the class of functions $f_\lambda(x) \in \mathcal{F}$ for all λ in $[0, 1]$. Let $F(x) \in \mathcal{F}$ and $F(x_c) = F_{\max} \leq b$. The parametric function f_λ can be expressed as follows:

$$f_\lambda(x) = \lambda F(x),$$

which implies $f_\lambda(x_c) = \lambda F_{max}$, which is the maximum value of $f_\lambda(x)$. A first consequence of this is Theorem 3 in [Wu04], which is a corollary of Theorem 3.3.1.



(a) $\lambda = 3.4$

(b) $\lambda = 3.6$

(c) $\lambda = 3.8$

(d) $\lambda = 4$

Figure 3.3: *GON* of the logistic map as a function of the initial condition for different values of λ and symbolic sequences of length $M = 16$.

Corollary 3.4.1 ([Wu04]). *For $f_\lambda(x) = \lambda F(x)$ with $F(x) \in \mathcal{F}$ and $\lambda \in [0, 1]$, it is satisfied that $GON(S_{f_\lambda}(f_\lambda(x))) \leq GON(S_{f_\lambda}(f_\lambda(x_c))), \forall x \in [a, b]$.*

Moreover, the maximum value of $f_\lambda(x)$, i.e., $\lambda F_{\max}$ depends on λ in such a way that an increment of the control parameter forces an increment of the maximum value. As a consequence, the GON of the kneading sequences derived from $x = f_\lambda(x_c)$ is an increasing function with respect to the control parameter [Wu04, Theorem 4].

Corollary 3.4.2 ([Wu04]). *For $f_\lambda(x) = \lambda F(x)$ with $F(x) \in \mathcal{F}$ and $\lambda_1, \lambda_2 \in [0, 1]$ with $\lambda_1 < \lambda_2$, it is satisfied that $GON(S_{f_{\lambda_1}}(f_{\lambda_1}(x_c))) \leq GON(S_{f_{\lambda_2}}(f_{\lambda_2}(x_c)))$.*

For the sake of clarity, the *GON* of the image of the critical point of the logistic map was calculated for different values of the control parameter. In Fig. 3.4 the results are depicted, confirming Corollary 3.4.2.

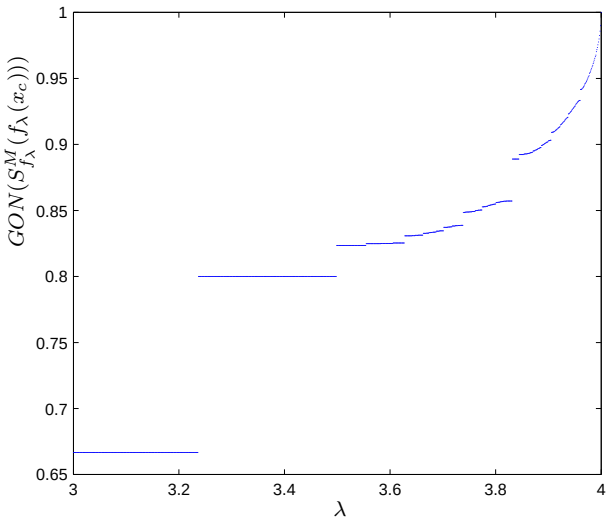


Figure 3.4: Maximum GON for the logistic map with respect to λ. The length of the symbolic sequences is $M = 16$.

On the other hand, after a certain number of transient iterations, all the values obtained from any initial condition through the iteration of any function in $\mathcal{F}$ are inside the interval $[x_{\min}, x_{\max}]$. Therefore, once all the values derived from the iteration of the considered function are inside $[x_{\min}, x_{\max}]$, it is verified that $GON(S_{f_\lambda}(x)) \geq GON(S_{f_\lambda}(f^{(2)}_\lambda(x_c))$. This was wrongly interpreted in [Wu04, Theorem 5], since this theorem is only satisfied if $f^{(2)}_\lambda(x) \geq x_{\min}$ for any $x \in [a, b]$. Nevertheless, the previous comments point out that this inequality is verified only for $x \in [f^{-1}_\lambda(f^{-1}_\lambda(x_{\min})), b]$, i.e., Theorem 5 in [Wu04] is not fulfilled for $x \in [a, f^{-1}_\lambda(f^{-1}_\lambda(x_{\min}))]$. Consequently, it is necessary to modify Theorem 5 in [Wu04] according to the preceding considerations. In this sense, the next corollary rewrites Theorem 5 in [Wu04] in a more accurate way and, at the same time, extends its application domain to all the functions in $\mathcal{F}$.

Corollary 3.4.3. *Let $F(x)$ be a function in $\mathcal{F}$ that leads to $f_\lambda(x) = \lambda F(x)$ for $x \in [a, b]$ and $\lambda \in [0, 1]$. Let x_i be defined as $x_i = x$ for $i = 0$ and $x_i = f_\lambda(x_{i-1})$ for $i > 0, i \in \mathbb{N}$. There exists $n_1 \in \mathbb{N}$ such that x_i is in $[x_{\min}, x_{\max}]$ for $i > n_1$ and it is satisfied that $GON(S_{f_\lambda}(x_i)) \geq GON(S_{f_\lambda}(f^{(2)}_\lambda(x_c)), \forall x \in [a, b]$ for $i > n_1$.*

Finally, the value $x_{\min}$ is given by $f^{(2)}_\lambda(x_c) = f_\lambda(f_\lambda(x_c)) = \lambda F(\lambda F_{\max})$. If $x_{\min}$ is a monotonic function of λ, then it is possible to extract a new corollary from Theorem 3.3.1. In [Wu04, Theorem 6] it is assumed without proof that $f^{(2)}_\lambda(x_c)$ is a monotonic decreasing function with respect to λ. This assumption implies that

$$\frac{\partial x_{\min}}{\partial \lambda} = F(\lambda F_{\max}) + \lambda F_{\max} \left.\frac{\partial F(x)}{\partial x}\right|_{x=\lambda F_{\max}} < 0. \tag{3.5}$$

This condition is not satisfied for all the possible values λ and for all the functions in $\mathcal{F}$. In [Wu04] the dependency of $x_{\min}$ on λ is studied using the logistic map (see Eq. (1.9)). It is easy to verify that for the logistic map the condition given by Eq. (3.5) is fulfilled if and only if $\lambda > 8/3$. Therefore, Theorem 6 in [Wu04] must be rewritten in such a way that the discussed inaccuracy is overcome and, simultaneously, the application domain of its variant affects not only to the logistic map but to all the functions in $\mathcal{F}$. Again, this aim is completed through a series of additional assumptions on the scope defined in Theorem 3.3.1.

Corollary 3.4.4. *Let us suppose that* $f_\lambda(x) = \lambda F(x)$ *with* $F(x) \in \mathcal{F}$, $\lambda \in [0,1]$ *and* $x \in [a,b]$. *For* $\lambda_1, \lambda_2 \in [0,1]$ *with* $\lambda_1 < \lambda_2$ *and satisfying* $\partial f_\lambda^{(2)}(x_c)/\partial\lambda < 0$ *for* $\lambda = \{\lambda_1, \lambda_2\}$, *it is verified that* $GON(S_{f_{\lambda_1}}(f_{\lambda_1}^{(2)}(x_c))) \geq GON(S_{f_{\lambda_2}}(f_{\lambda_2}^{(2)}(x_c)))$.

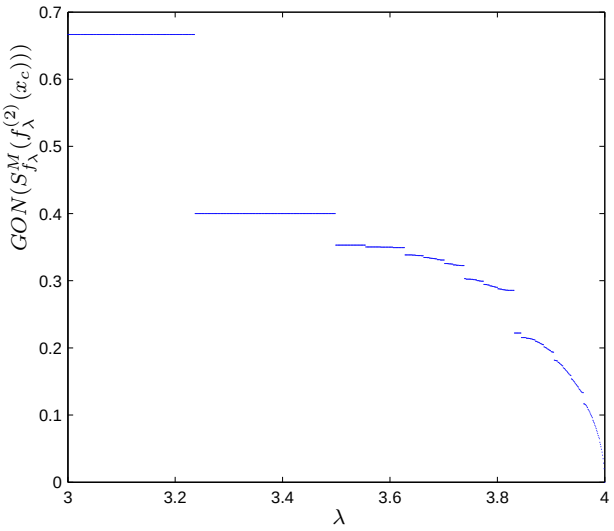


Figure 3.5: Minimum value of the GON of the logistic map. The length of the symbolic sequences is $M = 16$.

In order to illustrate the last two corollaries, the corresponding simulations were done on the logistic map. In Fig. 3.5 it is shown the GON of the symbolic sequences obtained by iterating the logistic map from the image of its critical point. Additionally, the bifurcation diagram of the GON of the logistic map was computed and the result is shown in Fig. 3.6. A first sight of this figure informs about the existence of two bounds, an upper and lower bound of the bifurcation diagram. It can be straightforwardly verified that the upper bound corresponds to Fig. 3.4 (which confirms Corollary 3.4.1), whereas the lower bound is given by Fig. 3.5 (which confirms Corollary 3.4.4).

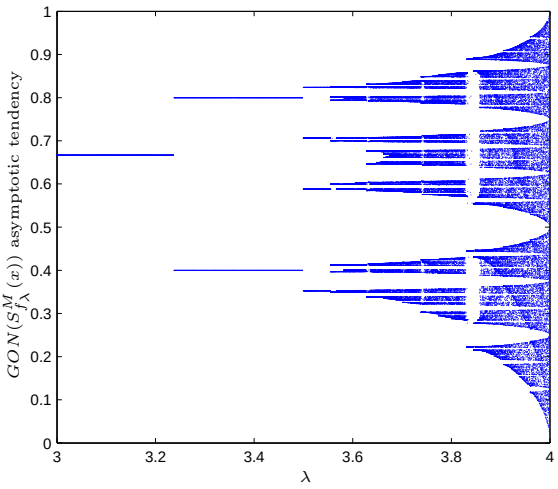


Figure 3.6: Bifurcation diagram of the GON of the logistic map. The length of the symbolic sequences is $M = 16$.

3.5 Application of Gray codes to initial condition and control parameter estimation

As it has been pointed out in the previous section, the symbolic sequences of the maps in $\mathcal{F}$ can be ordered according to either the control parameter or the initial condition, which can be further used to estimate either the control parameter or the initial condition attained to a given symbolic sequence. First, according to Corollary 3.4.1, the maximum symbolic sequence of a map in $\mathcal{F}$ is obtained from an initial condition equal to the image of the critical point. In the case of maps defined in a parametric way, the maximum symbolic sequence increases as λ does. Consequently, it is possible to establish a method to estimate the control parameter from a given symbolic sequence [Wu04]. In this regarding, it is assumed that the symbolic sequence is given by the first M symbols of the symbolic sequence generated from $x_0 \in \mathcal{U}$ through the iteration of a unimodal map $f_\lambda : \mathcal{U} \to \mathcal{U}$ included in $\mathcal{F}$. Let us define $G_M(x_0, \hat{\lambda}) = g_0 g_1 \cdots g_{M-1}$, $g_i \in \{0, 1\}$ as the Gray code generated from initial condition x_0, and control parameter $\hat{\lambda}$. The estimation of $\hat{\lambda}$ and x_0 from $G^M(x_0, \hat{\lambda})$ comprises three stages:

1. Estimation of the maximum GON contained in $G_M(x_0, \hat{\lambda})$ (see Fig. 3.7).
   According to [Guckenheimer79], if $\hat{\lambda}$ is selected implying chaotic behavior, then the probability density of the critical point x_c in the orbit generated from x_0 is nonzero. Therefore, if M is a large value, the maximum GON included in $G_M(x_0, \hat{\lambda})$ is the one obtained for initial condition equal to $f_{\hat{\lambda}}(x_c)$ (Coro-

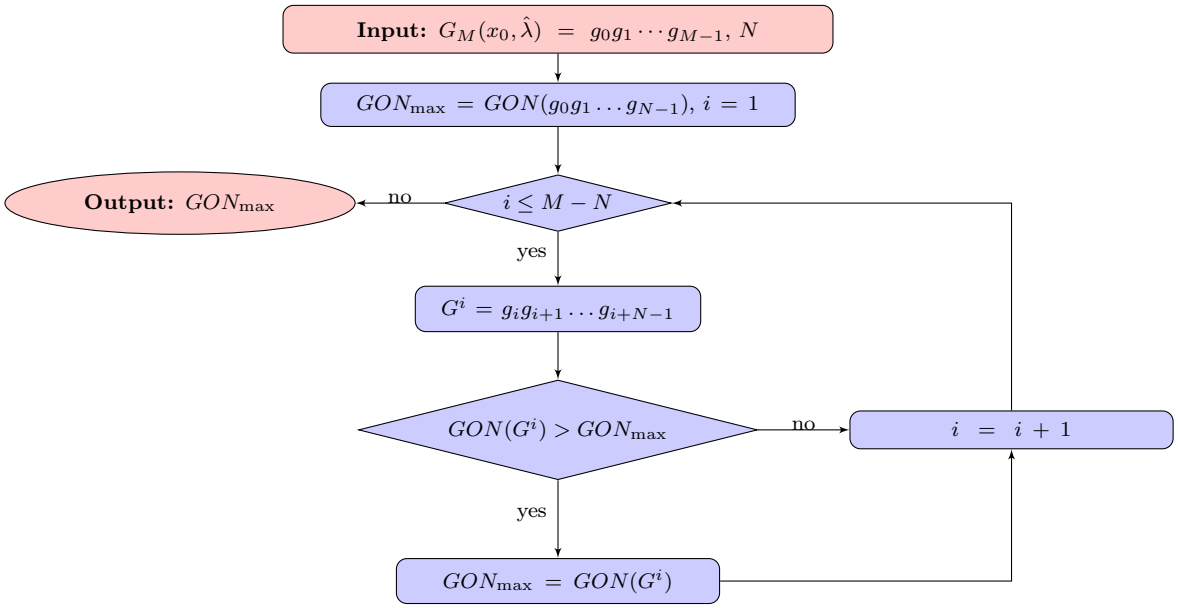


Figure 3.7: Estimation of the maximum GON contained in a Gray code associated to an unimodal map.

llary 3.4.1). As a result, the maximum GON can be calculated as the maximum GON of the $M - N + 1$ Gray codes obtained from $G_M(x_0, \hat{\lambda})$ using a sliding window of length N.

2. Recovering of the control parameter from the maximum GON.
   The GON of the Gray codes derived from the iteration of $f_\lambda \in \mathcal{F}$ with initial condition given by $f_\lambda(x_c)$ is an increasing function with respect to λ (Corollary 3.4.2). It means that it is possible to infer an estimation λ_{est} of $\hat{\lambda}$ from the $GON_{\max}$ obtained from $G_M(x_0, \hat{\lambda})$. Certainly, if λ_L and λ_R are the bounds of the interval containing $\hat{\lambda}$, then a dichotomic search of $\hat{\lambda}$ can be performed according to the monotony of $GON(G_N(f_\lambda(x_c), \lambda))$ (see Fig. 3.8).

3. Recovering of the initial condition x_0 using the value of the control parameter obtained in the previous stage.
   Gray codes of unimodal maps divide the state space $\mathcal{U}$ into a number of finite intervals. If Gray codes of length M are considered, the state space is split into 2^{M+1} different intervals. Therefore, given $\epsilon > 0$, any real number $x_0 \in \mathcal{U}$ can be represented with precision ϵ as a Gray code of $f_\lambda \in \mathcal{F}$, with initial condition x_0 and length above certain threshold [Stojanovski97]. Moreover, the Gray code assigned to any possible $x_0 \in \mathcal{U}$ increases as x_0 does. Accordingly, a dichotomic search of x_0 can be performed from $G_M(x_0, \hat{\lambda})$ as it is shown in Fig. 3.9. If one

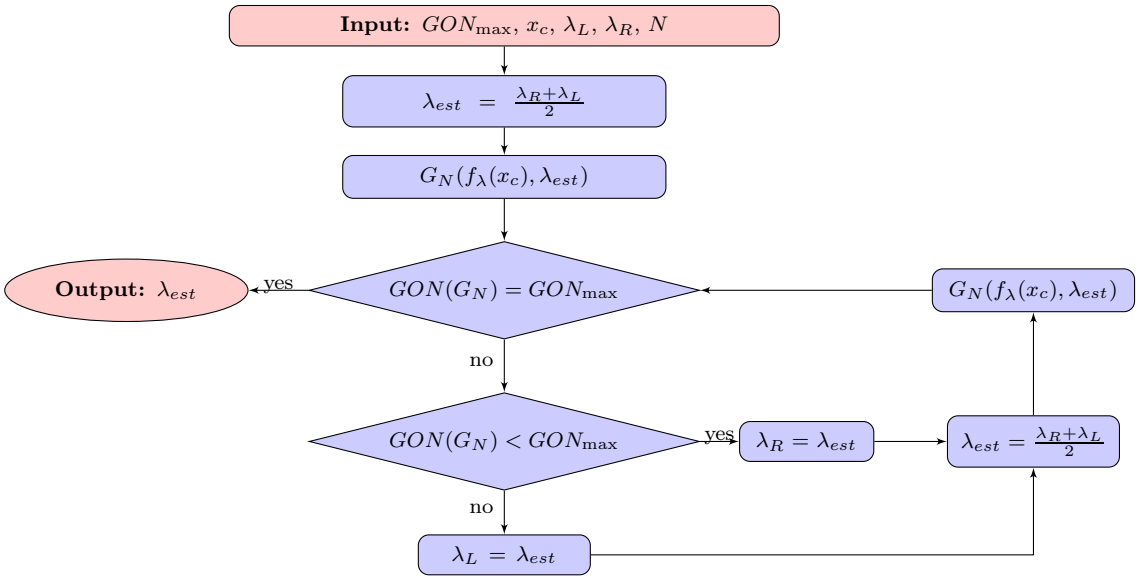


Figure 3.8: Algorithm for the estimation of the control parameter of an unimodal map from the maximum GON contained in a Gray code.

knows the exact value of $\hat{\lambda}$, then x_0 can be recovered up to a certain precision determined by M. On the other hand, if one has only access to an estimated value λ_{est} of $\hat{\lambda}$, then the estimated initial condition $x_{0_{est}}$ does not matched the actual value of x_0.

The precision in the estimation of both $\hat{\lambda}$ and x_0 depends critically on the first stage of the method. As it has been mentioned above, from a theoretical point of view the critical point x_c is included in almost every orbit when $\hat{\lambda}$ implies that $LE(\hat{\lambda}) > 0$ [Jensen85]. Nevertheless, in the context of finite precision computation this property is not satisfied, due to the digital degradation of the dynamics of chaotic systems. Therefore, the value $GON_{\max}$ obtained in the first step diverge from $GON(G_N(f_{\hat{\lambda}}(x_c), \hat{\lambda}))$, and thus the value λ_{est} obtained in second stage is not equal to $\hat{\lambda}$. As a matter fact, even for M very large, there exists an error that cannot be overcome. However, the value λ_{est} can be considered as a good estimation of $\hat{\lambda}$, which has to be later improved. Furthermore, in the context of chaos-based cryptography, it has serious consequences if the control parameter is part of the key.

Case study 3.5.1 ([Arroyo09f]). *Cryptanalysis of the cryptosystem introduced in [Wang08c]*

As an example, let us consider the cryptosystem defined in [Wang08c] and cryptanalyzed by us in [Arroyo09f]. This cryptosystem is a *searching based digital chaotic cipher*, i.e., it splits the plaintext into blocks that are further located in a binary

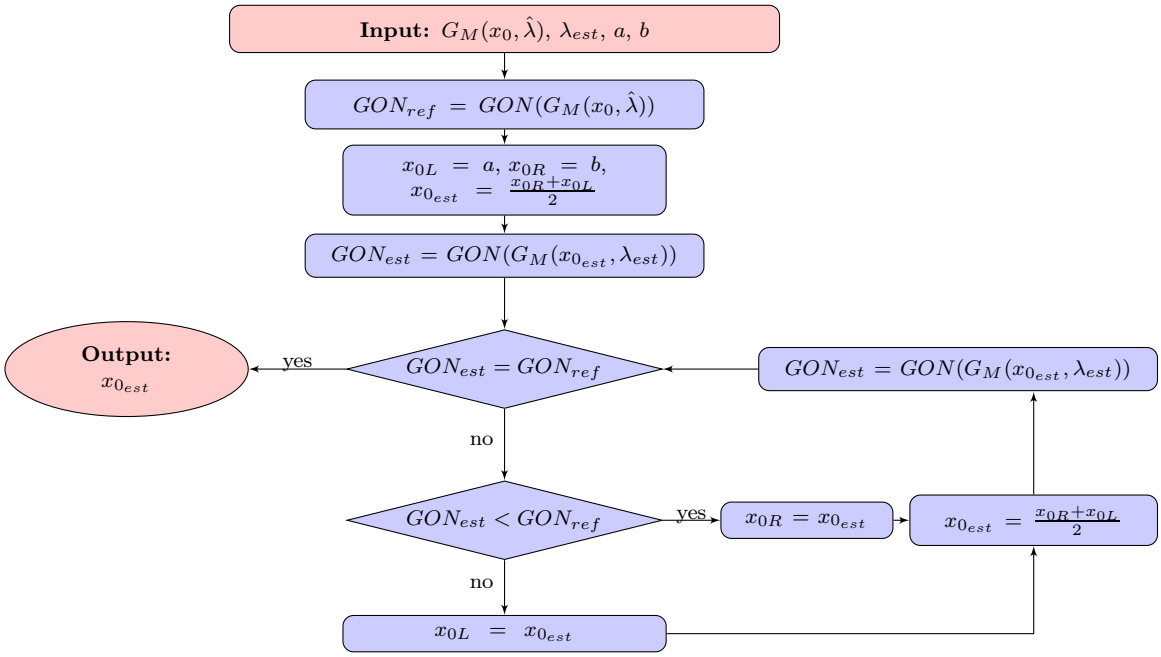


Figure 3.9: Algorithm for the estimation of the initial condition of an unimodal map from a given symbolic sequence when the control parameter is known.

sequence generated using a chaotic map. The authors of [Wang08c] claim that most chaotic systems can be used to generate the binary sequences required by the search based encryption procedure. Among all the possible options, the symbolic sequences of the logistic map were chosen in [Wang08c] to prove the reliability of the cryptosystem. In this sense, the secret of the cryptosystem is composed of the initial condition x_0 and the control parameter $\hat{\lambda}$, and the Gray code $G_M(x_0, \hat{\lambda}) = g_0 g_1 \cdots g_{M-1}$ is used to encrypt the plaintext P as follows:

- Step 1) Initialize $i = 0, j = 0$.
- Step 2) For the i-th plain block P_i formed by $w_i = w$ bits, try to find the first w_i-bit segment of $\{g_n\}_{n=j}^{N_{max}+w_i}$ which is equal to P_i; in case a segment is not found, let $w_i = w_i - 1$ and repeat this step. The parameter N_{max} indicates the maximum number of trials in the searching of P_i through the binary sequence.
- Step 3) Denoting by n_i the number of iterations needed to locate the distinguished w_i-bit segment from g_j, output (w_i, n_i) as the i-th cipher-block.
- Step 4) Set $i = i + 1$ and $j = j + n_i + w_i$, then go to Step 2 until the whole plaintext is exhausted.

According to the theory of symbolic dynamics of maps in $\mathcal{F}$, as long as one can reconstruct the sequence $G_M(x_0, \hat{\lambda})$, one can estimate the secret key of the cryptosystem. This is used to build an attack with three different stages:

1. Reconstruction of the Gray code derived from the logistic map.
   If one has access to the decryption machine, then one can perform a chosen-ciphertext attack to reconstruct $G_M(x_0, \hat{\lambda})$, i.e., the Gray code associated to the values of x_0 and $\hat{\lambda}$ that make up the secret key of the cryptosystem under consideration. To do so, L ciphertexts are generated as $(w, w \cdot i)$ for $i = 0, 1, 2, \ldots, L$. As an example, let us assume that $x_0 = 1/2$ and $\hat{\lambda} = 3.78$. In this case, it is satisfied that

   $$G_M(1/2, 3.78) = \{1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1 \ldots\}\,.$$

   As a result, if we ask the decryption machine to decrypt $(8, 0)$, then we obtain $\{1, 1, 0, 1, 1, 0, 1, 1\}$. Similarly, the decryption machine will return

   $$\{1, 0, 1, 1, 1, 1, 1, 0\}\,,$$

   when the input is $(8, 8)$, and $\{1, 1, 1, 1, 0, 1, 1, 1\}$ when the input is $(8, 16)$. In other words, the decryption of the first ciphertext returns the first w bits of $G_M(x_0, \hat{\lambda})$, the decryption of the second ciphertext gives the second set of w bits of $G_M(x_0, \hat{\lambda})$, and so on.

2. Estimation of the control parameter from the reconstructed Gray code.
   Once $G_M(x_0, \hat{\lambda})$ is known, the control parameter can be estimated as λ_{est} applying first the procedure explained in Fig. 3.7 (with $\lambda_L = 3.5$, $\lambda_R = 4$, and $x_c = 1/2$), and second the algorithm described in Fig. 3.8. In order to test the precision in the recovering of the control parameter, some simulations have been carried out. The parameter estimation errors for $\hat{\lambda} = 3.919740$ are shown in Fig. 3.10. Different values of x_0 and M were considered, for a fixed length of the subsequences of $N = 100$. Figure 3.10 spells out that the error in the estimation of $\hat{\lambda}$ decreases as M increases. Nevertheless, there exists an underlying error that it is impossible to overcome increasing M. Indeed, the exact value of $\hat{\lambda}$ can be only recovered if the orbit generated from x_0 using $\hat{\lambda}$ includes x_c, which it is satisfied theoretically but not when working with finite precision arithmetics. Anyhow, the proposed method allows to obtain an estimation λ_{est} of $\hat{\lambda}$ which implies a considerable narrowing of the key space, and which can be further improved through a trial and error strategy, i.e., a brute force attack on the value of the control parameter in a drastically reduced key-space.

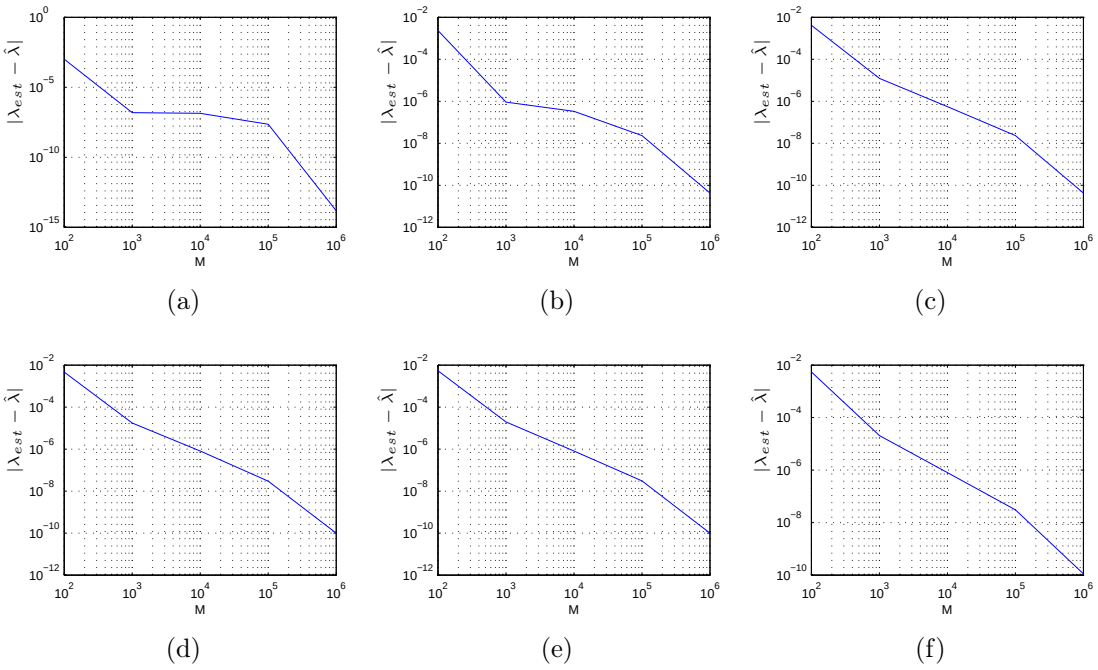


Figure 3.10: Parameter estimation error for $\hat{\lambda} = 3.919740$, different values of x_0 and M. The length of the symbolic subsequences is $N = 100$. The error is calculated as $|\lambda_{est} - \hat{\lambda}|$. Logarithmic scales are used for both the X- and Y- axes.

3. Estimation of the initial condition from the reconstructed Gray code and the estimated control parameter.

   When considering the security of a cryptosystem, a partial knowledge of the key must not lead to the determination of the rest of the key [Alvarez06b, Rule 7]. Therefore, even if we were not able to estimate the value of $\hat{\lambda}$ and obtain the exact value through a brute-force attack, the recovery of x_0 based on the knowledge of the other subkey $\hat{\lambda}$ would represent a very important flaw of the cryptosystem under study. This being the case, the algorithm described in Fig. 3.9 can be used to estimate the value of x_0 from $G_M(x_0, \hat{\lambda})$ and $\hat{\lambda}$. The results are shown in Fig. 3.11. For all analyzed situations, a number of bits greater than 80 implies an estimation error below 10^{-15}. Since all the simulations were performed using double precision, this means that the exact recovery of the initial condition is possible.

3.6 Concluding remarks

In this Chapter it has been shown that it is possible to get an estimation of the control parameter and the initial condition of a unimodal map from a given symbolic

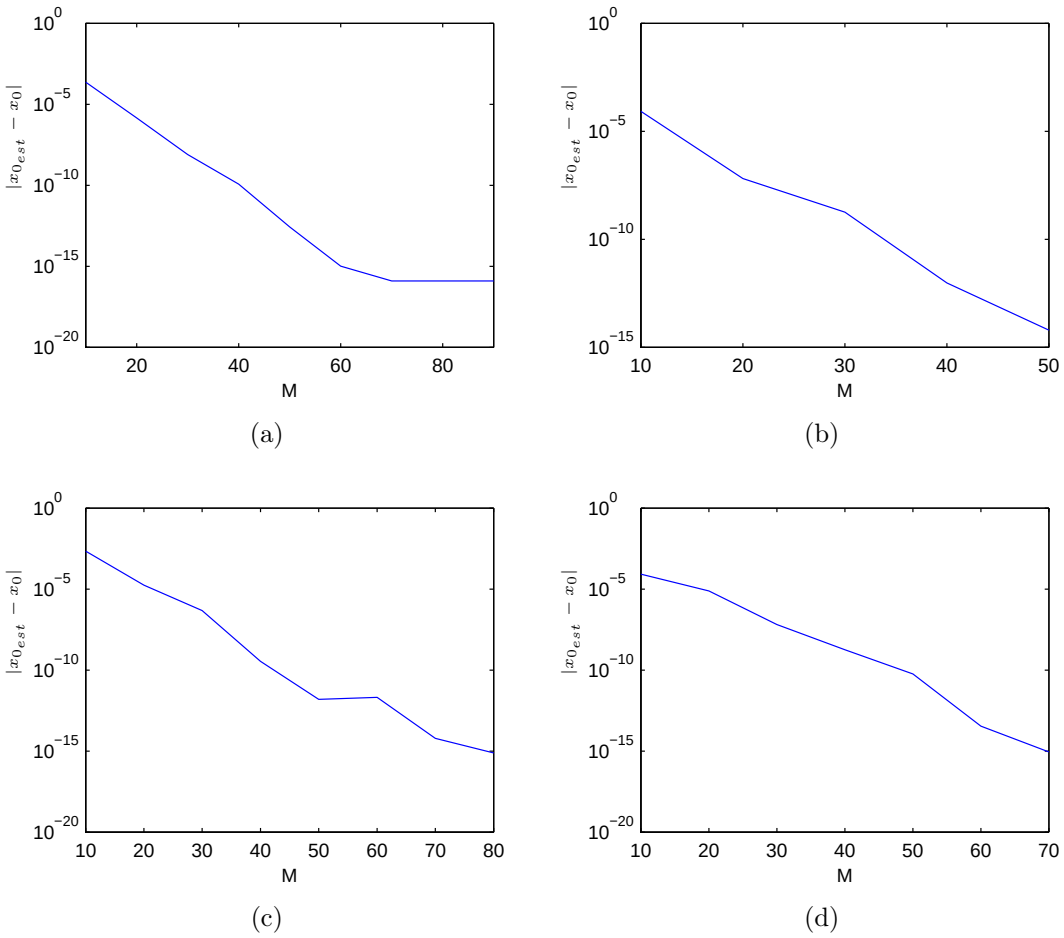


Figure 3.11: Initial condition estimation errors for different values of M and (a) $\hat{\lambda} = 3.950102, x_0 = 0.119372$; (b) $\hat{\lambda} = 3.950102, x_0 = 0.738197$; (c) $\hat{\lambda} = 3.791937, x_0 = 0.119372$; (d) $\hat{\lambda} = 3.791937, x_0 = 0.738197$. The minimum estimation error is bounded by the machine precision. Logarithmic scale is used for the Y- axis.

sequence. Moreover, if the control parameter of the unimodal map is known, then it is possible to perfectly recover the value of the initial condition. The possibility of performing such estimation (or recovering in the case of the initial condition) informs about serious problems related to cryptography. Indeed, if a unimodal map is used as base of a cryptosystem, then the encryption architecture must guarantee that there does not exist a meaningful leakage of the symbolic sequences of the underlying chaotic map. If it is possible to infer or build up symbolic sequences from the ciphertext, then an attacker could perform some kind of attack to derive a symbolic sequence large enough to get a good approximation of either the control parameter, or the initial condition, or both. This is the case of the cryptosystem analyzed in [Arroyo09f]. In this cryptanalytical work we have shown that unimodal maps are not

convenient for designing searching based digital chaotic ciphers. Indeed, if that encryption arquitecture is used along with an unimodal map, then a chosen-ciphertext attack can be performed to get the symbolic sequence corresponding to the secret key, i.e., the pair of values given by the initial condition and the control parameter. Once the symbolic sequence is obtained, the estimation of the secret key can be done straightforwardly. Nevertheless, the estimation of the control parameter can only be fulfilled if the maximum subsequence of a given symbolic sequence is obtained. For the class of unimodal maps considered in this Chapter the maximum symbolic sequence is obtained when the initial condition is the image of the critical point. Accordingly, the value of the control parameter can be found by comparing the maximum symbolic sequence to the symbolic sequences obtained from the image of the critical point and the control parameter ranging in its definition interval. Therefore, the critical point must be known and it can not be dependent on the control parameter. This is not the case of the skew tent map, whose critical point is equal to the control parameter being the image of the critical point constant. This situation is studied in the next Chapter, and an estimation method is proposed based on the concept of *order patterns*.

Chapter 4

Order patterns of unimodal maps

4.1 Introduction

Orbits of chaotic maps can be further transformed and analysed to bring to light the underlying and basic order, i.e., we can continue "twisting the lion's tail". According to Sharkovsky Theorem [Brin03, p. 162], order and dynamics are intertwined in one-dimensional intervals. It is therefore not surprising that the study of the ordinal structure of deterministic time series gives valuable information on the underlying dynamical system [Keller03; Keller04; Keller05; Keller07; Bandt05; Bandt07]. In the case of one-dimensional dynamical systems, that study can be performed by means of of their *order patterns* [Amigó06]. Indeed, order patterns allow to distinguish chaos from white noise [Amigó07c], and can provide useful information on the parameter or parameters controlling the dynamic of chaotic systems. The main goal of this Chapter is to estimate the control parameter of unimodal maps by means of their order patterns alone, even when the exact values of their orbits are not accessible but only the corresponding Gray codes.

Possible applications include the cryptanalysis of chaotic stream ciphers, which is a topic currently under investigation. More generally, real time series (like experimental observations or numerical simulations) are always coarse-grained versions of the actual values, on account of the finite precision of observational devices and computer arithmetic. This being the case, this Chapter touches upon a basic and difficult problem, if in a simplified setting.

This Chapter is based on the research work that we have carried out in [Arroyo09a; Arroyo09b], and is organized as follows. In Sec. 4.2, the concept of order pattern is introduced, and its dependence on the control parameter is analyzed for the logistic and the skew tent maps. How the order patterns of unimodal maps are obtained using Gray codes is explained in Sec. 4.3; in Sec. 4.4 it is explained how to use order patterns

to estimate the control parameter of unimodal maps with critical point depending on the control parameter. The results presented in this Chapter are summarized in Sec. 4.5, where some final comments are also included.

Table 4.1: Order patterns of length four.

#	Order pattern	#	Order pattern	#	Order pattern	#	Order pattern
0	[0, 1, 2, 3]	1	[0, 1, 3, 2]	2	[0, 3, 1, 2]	3	[3, 0, 1, 2]
4	[3, 0, 2, 1]	5	[0, 3, 2, 1]	6	[0, 2, 3, 1]	7	[0, 2, 1, 3]
8	[2, 0, 1, 3]	9	[2, 0, 3, 1]	10	[2, 3, 0, 1]	11	[3, 2, 0, 1]
12	[3, 2, 1, 0]	13	[2, 3, 1, 0]	14	[2, 1, 3, 0]	15	[2, 1, 0, 3]
16	[1, 2, 0, 3]	17	[1, 2, 3, 0]	18	[1, 3, 2, 0]	19	[3, 1, 2, 0]
20	[3, 1, 0, 2]	21	[1, 3, 0, 2]	22	[1, 0, 3, 2]	23	[1, 0, 2, 3]

4.2 Order patterns

For a given map defined as in Eq. (2.1), orbits $\gamma^+_{f_\lambda}(x_0)$ are calculated for any initial condition $x_0 \in \mathcal{U}$ according to Eq. (2.2). Orbits are used to define *order ν-patterns* (or order patterns *of length* ν), which are permutations of the elements $\{0, 1, ..., \nu-1\}$, $\nu \geq 2$. We write $\pi = [\pi_0, \pi_1, \ldots, \pi_{\nu-1}]$ for the permutation $\pi_0 \mapsto 0, ..., \pi_{\nu-1} \mapsto \nu - 1$.

Definition 4.2.1 (Order pattern)**.** *The point $x \in \mathcal{U}$ is said to define (or realize) the order ν-pattern $\pi = \pi(x) = [\pi_0, \pi_1, \ldots, \pi_{\nu-1}]$ if*

$$f^{\pi_0}(x) < f^{\pi_1}(x) < \ldots < f^{\pi_{\nu-1}}(x). \tag{4.1}$$

Alternatively, x is said to be of type π. The set of all possible order patterns of length ν is denoted by $\mathcal{S}_\nu$.

For further reference, it is convenient to assign an integer number to each order pattern. This can be made, for instance, by means of the Trotter-Johnson algorithm [Kreher98]. The order patterns of length 4 along with their "ordering numbers", are shown in Table 4.1.

As emphasized in [Amigó08b], there always exist order ν-patterns with sufficiently large ν that are not realized in any orbit of $f \in \mathcal{F}$. These order patterns are called *forbidden patterns*, whereas the rest of order patterns are called *allowed patterns*. 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

$$P_\pi = \{x \in \mathcal{U} : x \text{ is of type } \pi\}, \tag{4.2}$$

where $\pi \in \mathcal{S}_\nu$, 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. Remember that $f_\lambda : \mathcal{U} \to \mathcal{U}$ is said to be ergodic with respect to the invariant measure μ if the only invariant sets are the empty set and the full state space $\mathcal{U}$, except possibly for a μ-null set. According to Birkhoff's ergodic theorem [Walters82, 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. Being the scope the family of maps given by Definition 1.3.3, in the following two subsections this study is done experimentally with the logistic map (as representative of $\mathcal{F}_1$) and with the skew tent map (as representative of $\mathcal{F}_2$). Since we are primarily interested in the relation between the probabilities $\mu(P_\pi)$ (or relative frequencies) of order patterns $\pi \in \mathcal{S}_\nu$ and the control parameter λ of the map considered, we will refer to it as the λ-distribution function (in short: λ-DF) of π, since they are related to the probability distribution functions (we fix π instead of fixing λ).

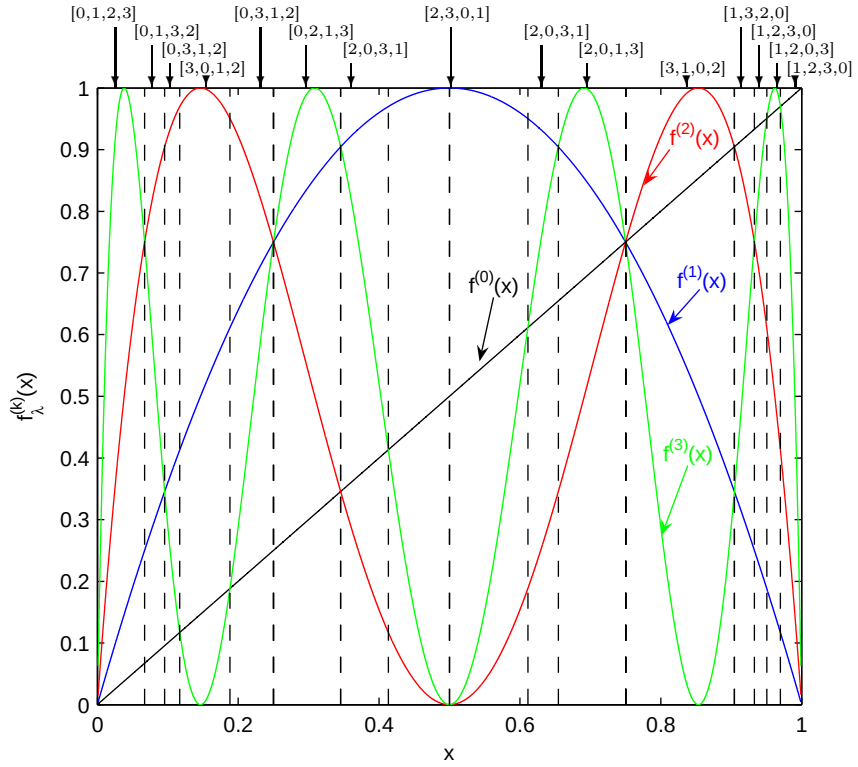


Figure 4.1: $f^{(k)}_\lambda(x)$ for $k = 0, 1, 2, 3$ and the corresponding order patterns of length 4 for the logistic map when $\lambda = 4$.

4.2.1 Order patterns for the logistic map

The logistic map, defined in Eq. (1.9), belongs to $\mathcal{F}_1$. The logistic map with $\lambda = 4$ was studied in [Amigó07c; Amigó08b] from the ordinal point of view. In Fig. 4.1 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.

However, the main goal of this Chapter is to analyze the relationship between the control parameter of maps in $\mathcal{F}_1$ or $\mathcal{F}_2$, and their order patterns, what calls for the distributions of allowed patterns for different values of λ. Figure 4.2 depicts the relative frequencies of each order 4-pattern for $\lambda \in [3.7, 4]$, the patterns being labeled as in Table 4.1. To be more specific, for every λ, a sufficiently long orbit was

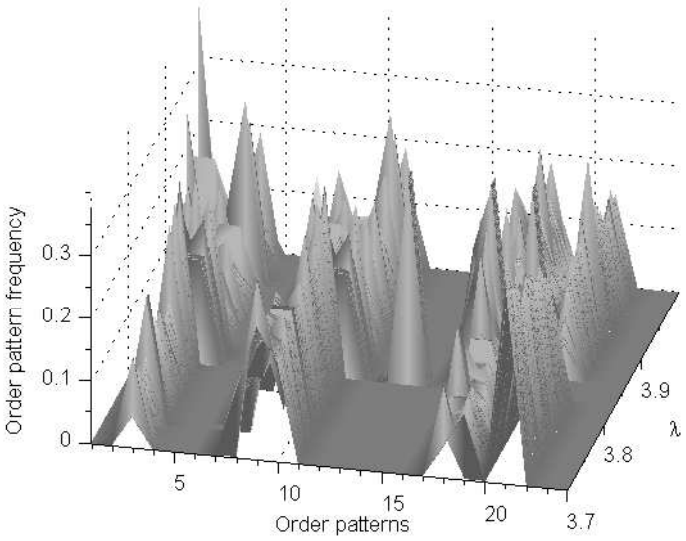


Figure 4.2: Relative frequency of the order patterns realized by the logistic map when $\nu = 4$ and $\lambda \in [3.7, 4]$.

generated, the occurrences of the different order patterns were counted using a sliding window of width 4, and finally the counts obtained were normalized by the number of windows. These results are estimates of the probabilities for the corresponding order patterns to occur. Let us point out that, since the physical invariant measure of the logistic map is only known for $\lambda = 4$, numerical estimation of those probabilities is the most we can hope for. More importantly for us, we conclude from Fig. 4.2 that it is very difficult to infer the value of $\lambda \in [3.7, 4]$ from the λ-DF of order patterns of length 4.

4.2.2 Order patterns for the skew tent map

The skew tent map, given by Eq. (1.11), belongs to the subclass $\mathcal{F}_2$, comprised of those maps of $\mathcal{F}$ parameterized by the critical point. Furthermore, for the skew tent map f_λ, the maximum value $f_\lambda(x_c) = f_\lambda(\lambda) = 1$ is independent from λ (see Fig. 1.9). The allowed order 4-patterns for the skew tent map are shown in Fig. 4.3 for $\lambda = 0.3$, and in Fig. 4.4 for $\lambda = 0.7$.

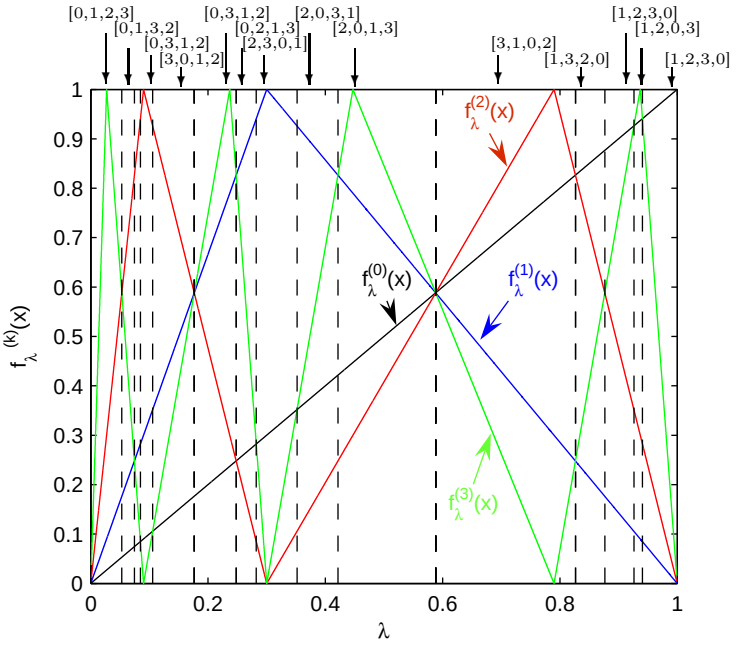


Figure 4.3: The first four iterations of $f(x)$ and the corresponding order patterns of length 4 for the skew tent map with $\lambda = 0.3$, i.e., $f_{0.3}^{(k)}(x)$ for $k = 0, 1, 2, 3$.

Contrarily to the logistic map, the skew tent map does possess a known ergodic invariant measure for all $\lambda \in (0, 1)$, namely, the Lebesgue measure on $[0, 1]$ (see [Billings01]). Hence, if P_π is given by Eq. (4.2) with $\mathcal{U} = [0, 1]$, 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. The easiest case corresponds to the order pattern $\pi = [0, 1, \ldots, \nu - 1]$, since then P_π is an open interval whose left endpoint is 0 and whose right endpoint is the leftmost intersection between $f_\lambda^{\nu-1}$ and $f_\lambda^{\nu-2}$. The relative frequencies of the order patterns of length 4, numbered according to Table 4.1, are depicted in Fig. 4.5. In particular, the length of the interval $P_{[0,1,2,3]} = (0, \phi_4(\lambda))$ is determined by the first intersection between $f_\lambda^{(2)}(x)$ and $f_\lambda^{(3)}(x)$:

$$\phi_4(\lambda) = \frac{\lambda^2}{2 - \lambda}. \tag{4.3}$$

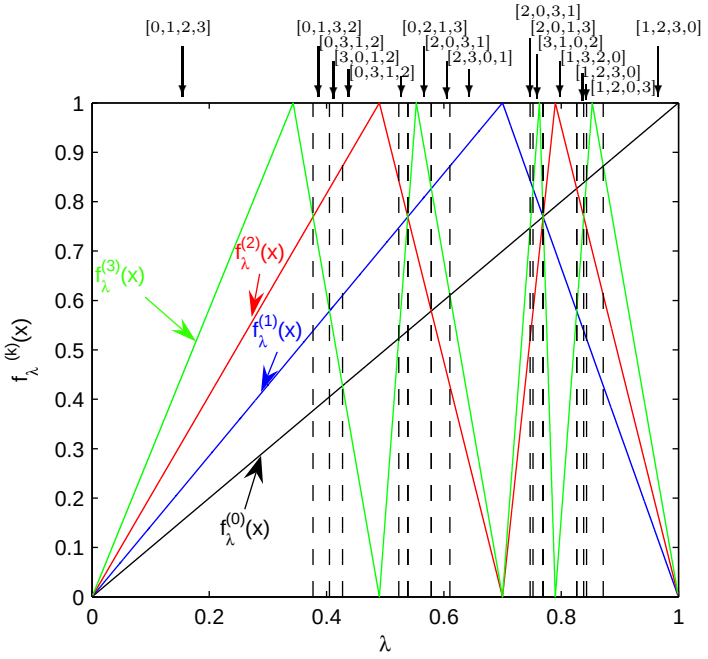


Figure 4.4: The first four iterations of $f(x)$ and the corresponding order patterns of length 4 for the skew tent map with $\lambda = 0.7$, i.e., $f_{0.7}^{(k)}(x)$ for $k = 0, 1, 2, 3$.

Therefore, the λ-DF of $\pi = [0, 1, 2, 3]$ (pattern #0) is given by $\phi_4(\lambda)$; see Fig. 4.6(a) for the graphical representation of $\phi_4(\lambda)$. The fact that the function $\phi_4(\lambda)$ is bijective entails the possibility of estimating λ via the relative frequency of the order pattern $[0, 1, 2, 3]$.

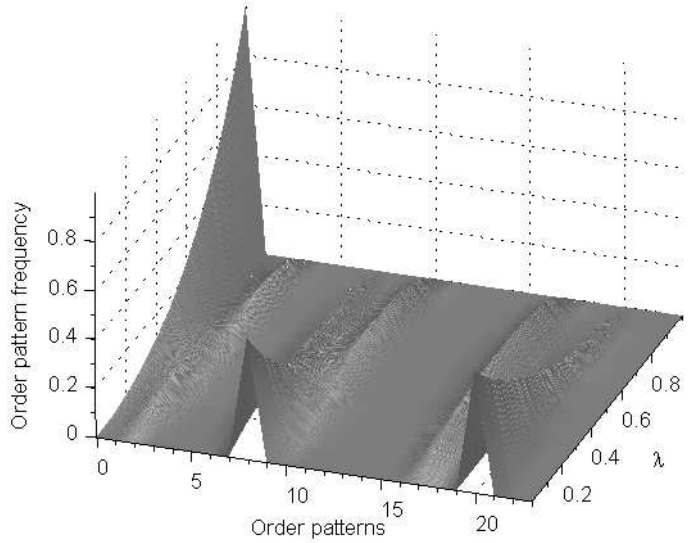


Figure 4.5: Relative frequencies of the order patterns of length $\nu = 4$ realized by the skew tent map.

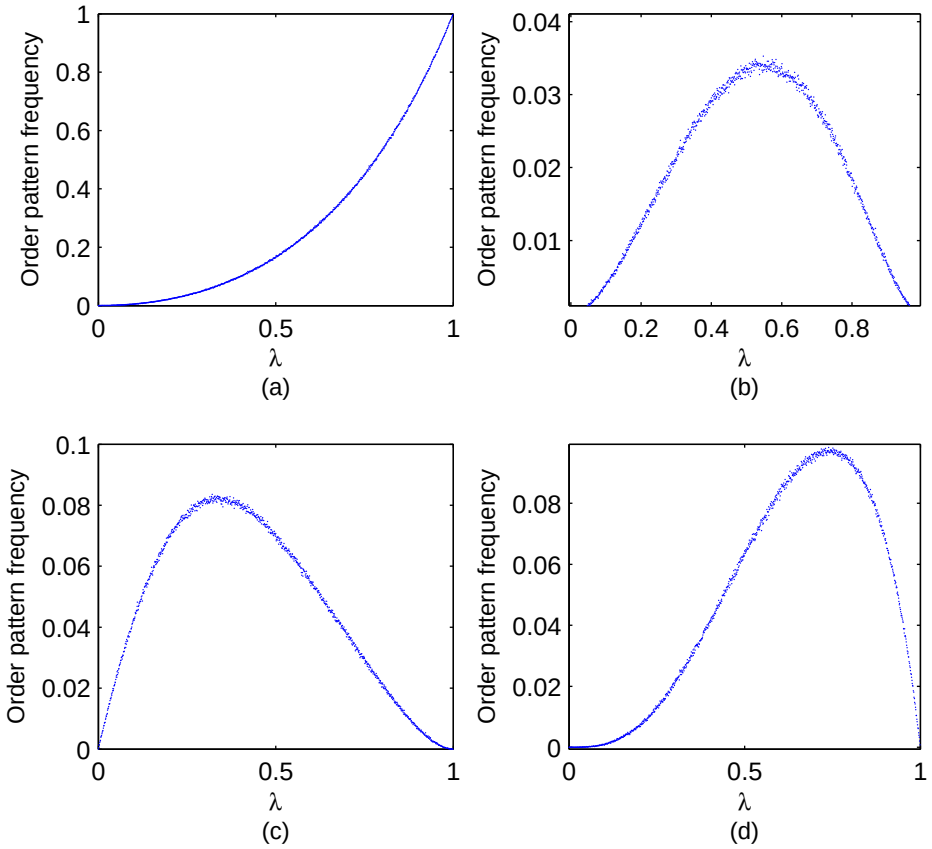


Figure 4.6: Order pattern frequency for the skew tent map and $\nu = 4$ (a) order pattern #0; (b) order pattern #1; (c) order pattern #2; (d) order pattern #3.

Up to this point it has been assumed that the orbits of the various maps considered, were accessible. From a more practical point of view, it is also relevant to know whether order patterns can be still determined using less information about the orbits. This is the case, for instance, when dealing with the symbolic dynamic associated to a generating partition of the state space. In particular, the orbits of maps of $\mathcal{F}$ can be transformed into binary sequences by the procedure described in Chapter 3. In the next section it is explained how to build order patterns from those binary sequences.

4.3 Gray codes and order patterns for unimodal maps

In this section the analysis focuses on the parametric unimodal maps of the subclasses $\mathcal{F}_1$ or $\mathcal{F}_2$. In section 4.2 it has been explained the dependence of the order patterns allowed for those maps with respect to the control parameter. Specifically, it has been estimated the probabilities of order 4-patterns by their relative frequencies in orbits

of the logistic map (Fig. 4.2) and of the skewed tent map (see Fig. 4.5) with different parameter settings. The next goal is to reproduce the same dependencies not from the exact values of the orbit point ("sharp orbit"), but from the binary sequence built as explained in Chapter 3 ("coarse-grained orbit"). Accordingly, the definition domain $\mathcal{U}$ of $f \in \mathcal{F}$ splits in 2^{M+1} subintervals when Gray codes of length M are considered. We show next that the order patterns of f can also be obtained comparing Gray codes obtained from its orbits.

Let $G_M(f,x) = g_0 g_1 \dots g_{M-1}$, $g_i \in \{0,1\}$, be the Gray code of length M of $x \in \mathcal{U}$. Since the Gray codes, together with the points $x \in \mathcal{U}$, are linearly ordered and, as we saw, their order relations are equivalent, we can expect to obtain useful information about the order patterns realized by the sharp orbit $\gamma_f^+(x)$ from the order patterns realized by the coarse-grained orbit $G_M(f,x)$, $M \geq 2$. The procedure is as follows.

1. Divide the Gray code of length M, $G_M(f,x)$, into $M-N+1$ Gray codes of length $N < M$ using a sliding window of length N. Thus, the first Gray code derived from $G_M(f,x)$ is $G^0 = g_0 g_1 \dots g_{N-1} = G_N(f,x)$, the second Gray code is $G^1 = g_1 g_2 \dots g_N = G_N(f,f(x))$, ..., and the $(M-N+1)$-th Gray code is $G^{M-N} = g_{M-N} g_{M-N+1} \dots g_{M-1} = G_N(f,f^{M-N}(x))$.

2. For $i = 0,1,...,M-N-\nu+1$, build groups of ν consecutive Gray codes $G^i G^{i+1} \dots G^{i+\nu-1}$. The i-th group defines then the order ν-pattern $\pi = \pi(i) = [\pi_0, \pi_1, \dots, \pi_{\nu-1}]$ if
$$G^{i+\pi_0} < G^{i+\pi_1} < \dots < G^{i+\pi_{\nu-1}}.$$

The order patterns derived using Gray codes need not have, in general, similar λ-DFs to those derived from the sharp orbits. Indeed, order patterns defined by Gray codes of length N are built upon the comparison of subintervals $I_j^{(N)} \subset \mathcal{U}$ (see Sect. 3.3), rather than comparing points of I. The width of the intervals $I_j^{(N)}$ decreases as the length N of the sliding window increases in such a way that when $N \to \infty$, each one of those intervals converges to a single real number. As a result, the error in the calculation of the order patterns from Gray codes is expected to reduce as N increases. In the context of finite-precision computation, the minimum value of N necessary to get a reliable approximation of the λ-DF of an order pattern is related to the precision of the arithmetic used. Again, this quantization error decreases as N increases and, consequently, a large value of N may be necessary to assure a good approximation of the λ-DF. Another source of divergences between λ-DFs and their numerical estimation via finite-length Gray codes are non-ergodicity or even poor ergodicity. As a matter of fact, remember that the estimation of the probability

$\mu(P_\pi)$ by the relative frequency of $\pi \in \mathcal{S}_\nu$ in finite orbits of a μ-preserving map, hinges on the ergodic theorem. If, furthermore, the convergence of relative frequencies to probabilities in the orbits of an ergodic map with respect to μ, is very slow, a good estimation would require exceedingly long sequences —this is what we mean by "poor ergodicity". These errors are shown in Figs. 4.7 and 4.8 for the logistic and the skew

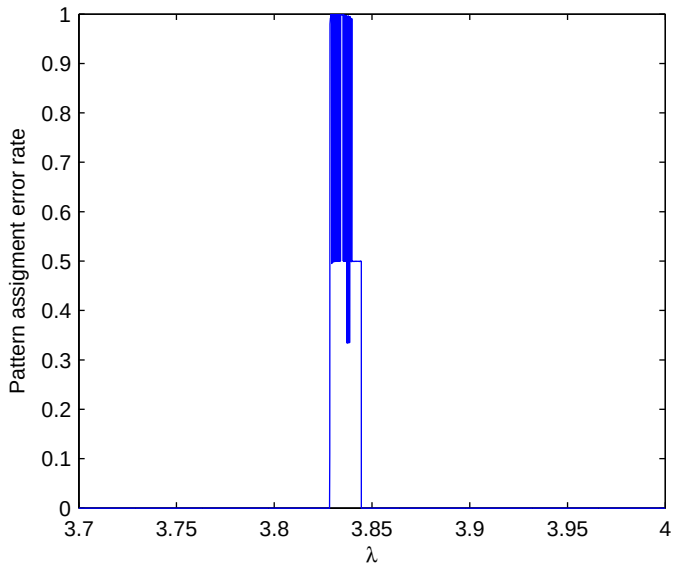


Figure 4.7: Error rate for the pattern assignment based on Gray codes with respect to the one based on the orbit of the logistic map. The length of order patterns is $\nu = 4$, the length of the considered Gray codes is $N = 100$ and the number of samples is 10104.

tent maps, respectively, with $\pi = [0, 1, 2, 3]$, $M = 10104$, and $N = 100$. In the first case, the value of λ lies within the period-3 window of the logistic map. In the second case, poor ergodicity is expected for values of λ close to 0 and 1. The asymmetry in the error distribution is due to the fact that for $\lambda \simeq 1$, the tent map looks like the identity in most of $\mathcal{U} = [0, 1]$, hence $P_{[0,1,2,3]}$ covers most of $\mathcal{U}$. This makes $[0, 1, 2, 3]$ to be the most frequent order 4-pattern even when its frequency is calculated using Gray codes. Comparison of Figs. 4.6 and 4.9 illustrates the accuracy of the Gray code-based method for the first four order 4-patterns (see Table 3.1) of the skew tent map.

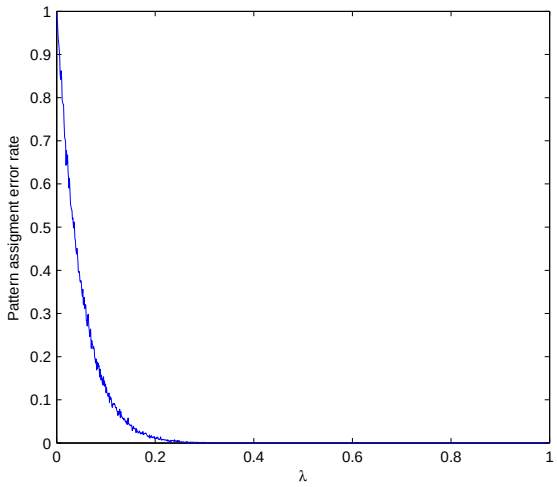


Figure 4.8: Error rate for the pattern assignment based on Gray codes with respect to the one based on the orbit of the skew tent map. The length of order patterns is $\nu = 4$, the length of the considered Gray codes is $N = 100$ and the number of samples is 10104.

4.4 Estimation of the control parameter for unimodal maps with critical point depending on the control parameter

The main characteristic of the maps in $\mathcal{F}_2$ is that the control parameter λ determines the value of the critical point. Furthermore, from the discussion above, it is expected that the relation between the control parameter and the allowed order patterns of the corresponding dynamic is specially simple for the pattern $\pi = [0, 1, ..., \nu - 1]$. Clearly, if the λ-DF of this pattern is 1-to-1, then λ can be pinpointed from that distribution function; otherwise, the possible values of λ can be reduced to a few candidates, which can also be acceptable in applications such as cryptanalysis. In turn, λ-DFs can be approximated via Gray codes, without previous knowledge of the critical point of the map. The bottom line is that the control parameter of a map in $\mathcal{F}_2$ can be estimated from their coarse-grained orbits (in form of Gray codes). The specifics depend on the map.

In more general terms, let $f_\lambda \in \mathcal{F}_2$ and suppose that each f_λ is ergodic for $\lambda \in \Lambda$ with the same invariant measure μ. Furthermore, assume that $f_\lambda(a) = a$, and $x < f_\lambda(x)$ on a maximal interval $(a, c) \subset (a, x_c)$. We claim that the interval

$$I_\nu^\lambda = (a, c) \cap f_\lambda^{-1}(a, c) \cap \ldots \cap f_\lambda^{-(\nu-1)}(a, c), \tag{4.4}$$

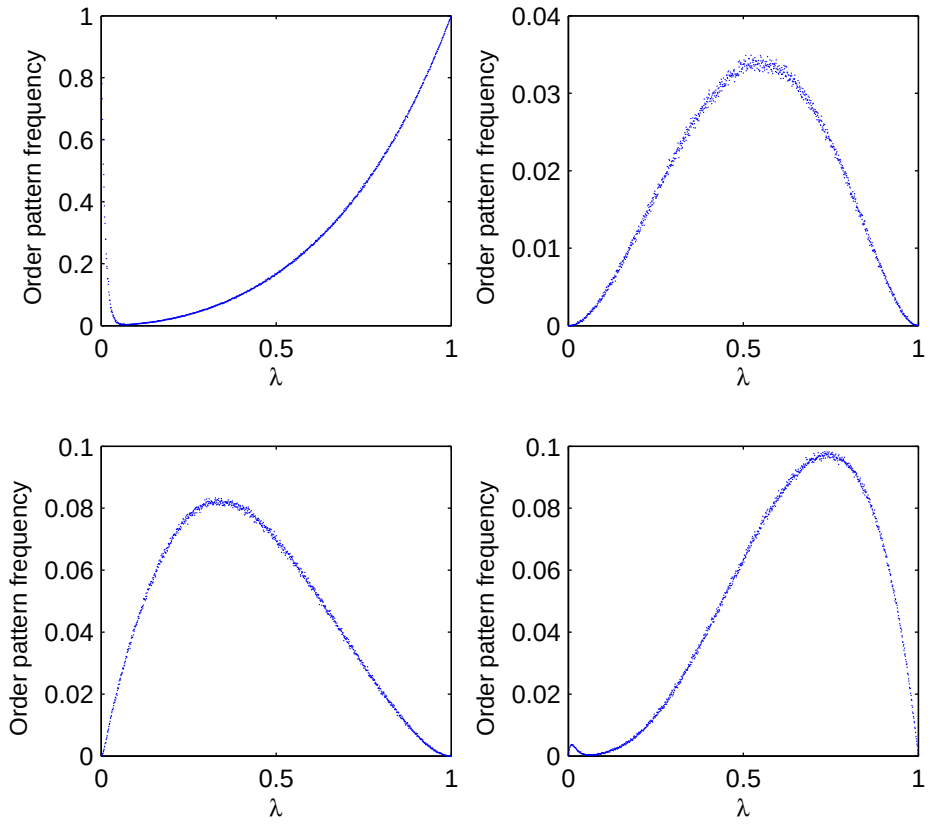


Figure 4.9: Relative frequency of order patterns of the skew tent map using Gray codes, when $\nu = 4$, $N = 100$ and the sequences are 10104-bit long: (a) order pattern #0; (b) order pattern #1; (c) order pattern #2; (d) order pattern #3.

coincides with $P_{[0,1,\ldots,\nu-1]}$. Indeed, if $x \in I_\nu^\lambda$, then $f^i(x) \in (a, c)$ for $0 \leq i \leq \nu - 1$, and

$$x < f_\lambda(x) \Longrightarrow f_\lambda(x) < f_\lambda^2(x) \Longrightarrow \ldots \Longrightarrow f_\lambda^{\nu-2}(x) < f_\lambda^{\nu-1}(x).$$

Hence, $I_\nu^\lambda \subset P_{[0,1,\ldots,\nu-1]}$. Conversely, if $x \in P_{[0,1,\ldots,\nu-1]}$, i.e.,

$$x < f_\lambda(x) < f_\lambda^2(x) < \ldots < f_\lambda^{\nu-1}(x),$$

then $f^i(x) \in (a, c)$ for $0 \leq i \leq \nu - 1$. Thus, $P_{[0,1,\ldots,\nu-1]} \subset I_\nu^\lambda$. This proves

$$P_{[0,1,\ldots,\nu-1]} = I_\nu^\lambda.$$

Because of ergodicity, the relative frequency at which a typical trajectory visits I_ν^λ is $\mu(I_\nu^\lambda)$. If $\mu(I_\nu^\lambda)$ happens different for each interval I_ν^λ, then $\mu(I_\nu^\lambda)$ can be used to determine or estimate the control parameter λ. In this case, the frequency of the order pattern $[0, 1, \ldots, \nu - 1]$ in an orbit $\gamma_{f_\lambda}^+(x)$ is just the number of times that

$f_\lambda^{i+j}(x) \in (a,c)$ for $i \in \mathbb{N} \cup 0$ and $j = 0, 1, \ldots, \nu-1$. As an example, consider the skew tent map again. For this map, the interval $P_{[0,1,\ldots,\nu-1]}$, i.e., the set of points $x \in [0,1]$ of type $[0,1,\ldots,\nu-1]$, is determined by the leftmost intersection of the iterates $f_\lambda^{\nu-2}$ and $f_\lambda^{\nu-1}$, where

$$f_\lambda^n(x) = \begin{cases} x/\lambda^n, & \text{if } 0 \le x \le \lambda^n \\ (\lambda^{n-1} - x)/\lambda^{n-1}(1-\lambda), & \text{if } \lambda^n \le x \le \lambda^{n-1} \end{cases} \tag{4.5}$$

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

$$\phi_\nu(\lambda) = \frac{\lambda^{\nu-2}}{2-\lambda}. \tag{4.6}$$

Since this function is 1-to-1 in the interval $0 \le \lambda \le 1$ for $\nu \ge 2$, with $\phi_2(0) = 1/2$, $\phi_{\nu\ge 3}(0) = 0$, and $\phi_{\nu\ge 2}(1) = 1$, it allows to estimate λ by estimating $\phi_\nu(\lambda)$ —the length of $P_{[0,1,\ldots,\nu-1]}$. Now, from the equation

$$\frac{d}{d\lambda}\phi_\nu(\lambda) \;=\; \frac{\lambda^{\nu-3}}{(2-\lambda)^2}[2(\nu-2) - (\nu-3)\lambda] = \begin{cases} 0, & \text{if } \lambda = 0 \\ \nu - 1, & \text{if } \lambda = 1 \end{cases} \tag{4.7}$$

it follows that $\phi_\nu(\lambda)$ is a $\cup$-convex function on $0 \le \lambda \le 1$ for $\nu \ge 2$, that converges to 0 on $0 \le \lambda < 1$ as $\nu \to \infty$. Therefore, the higher ν the worse $\phi_\nu(\lambda)$ discriminates different values of λ. Consequently, $\nu = 3, 4$ are the best choices for a quality estimation of λ.

On the other hand, the ergodicity of the skew tent map permits to estimate the length of $P_{[0,1,\ldots,\nu-1]}$ by estimating the relative frequency of the $\pi = [0,1,\ldots,\nu-1]$ in a typical sharp orbit of the map —or, as we intent, in a typical coarse-grained orbit. In the latter case, the choice for the parameter N, the width of the sliding window down the Gray codes (Sec. 4.3), must be also analyzed. The minimum value of N to get a good reconstruction of the λ-DF of the order patterns, N_{min}, depends on the precision of the arithmetic used, but it also depends on the Lyapunov exponent of the map. If floating point double-precision arithmetic is implemented, then N_{min} can be determined as function of λ by comparing pairs of symbolic sequences generated from the same initial condition, with control parameters λ_1 and λ_2 such that $|\lambda_2 - \lambda_1|$ equals the spacing of floating point numbers. Figure 4.10 shows the dependence of N_{min} with respect to λ.

Summing up, the estimation of the control parameter $\lambda \in (0,1)$ of the skew tent map f_λ, Eq. (1.11), can be done by counting and normalizing the occurrences of the order pattern $[0,1,...,\nu-1]$, ideally for $\nu = 3$ or 4, in a statistically significant sample of orbit segments of f_λ. This follows from the following properties: (i) f_λ is ergodic for all λ, and (ii) the f_λ-invariant measure of $P_{[0,1,\ldots,\nu-1]}$ (in this case, the

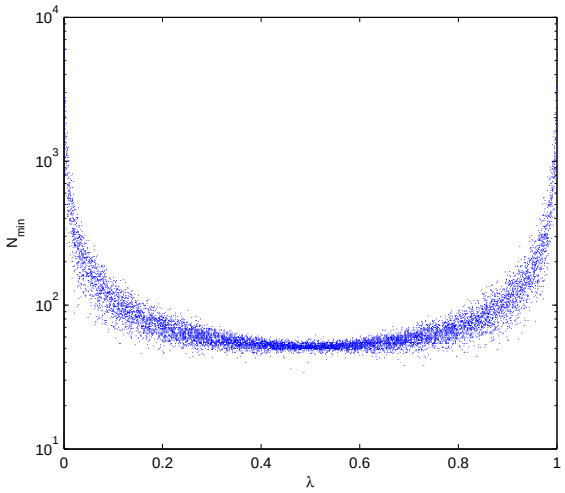


Figure 4.10: Minimum width of the sliding window necessary for the reconstruction of the PDF of the order patterns from the symbolic sequences of the skew tent map.

length of the interval $P_{[0,1,\ldots,\nu-1]}$) depends bijectively on λ. In a practical context though, finite precision machines are used, and this entails, in general, numerical degradation, meaning that the computed orbits, whether of chaotic or non-chaotic maps, depart from the real ones. In the case of a very long orbit of a chaotic map, the deviation of the numerical simulation (locally measured by the Lyapunov exponent of the map) will be severe; in such cases, it is preferable to have many shorter orbits instead. Even worse, all orbits computed with finite precision are eventually periodic. This distortion of the dynamics, due to finite numerical precision and dependence on initial conditions, implies the general impossibility of obtaining orbits and invariant measures in an exact way. As a matter of fact, all this carries over to symbolic dynamics.

To verify this issue in the case of coarse-grained orbits, a sample of Gray codes of the skew tent map, each one with the same length but with a different initial condition, was generated for every value of λ. The underlying sharp orbits were computed with double precision floating point arithmetic. From this sample of Gray codes, the corresponding λ-DFs of the order patterns of length $\nu = 4$ were obtained. The λ-DF of the order pattern $[0, 1, 2, 3]$ (#0 for short) was calculated as the mean value of the λ-DFs obtained from the various initial conditions. This average value is compared to the exact λ-DF, $\phi_4(\lambda) = \lambda^2/(2 - \lambda)$, in Fig. 4.11, along with the corresponding standard deviation.

Fig. 4.11 spells out that, in the context of finite precision computation, the perfect recovery of the control parameter value using the λ-DF of order pattern #0, is not

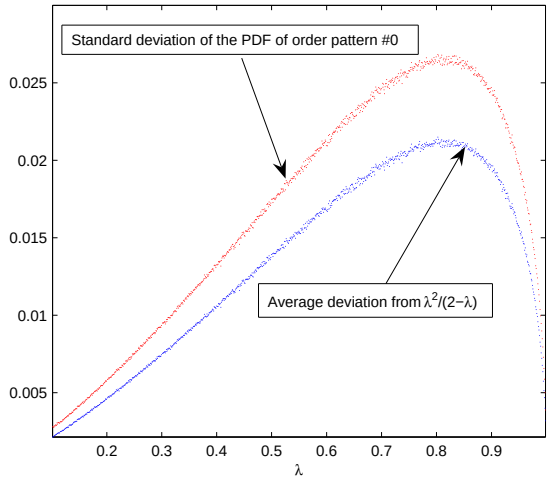


Figure 4.11: Average deviation and standard deviation in the estimation of the PDF of the order pattern #0 for the skew tent map with respect to $\lambda^2/(2-\lambda)$.

feasible in general if one can only resort to Gray codes. However, it is possible to locate λ up to an uncertainty interval. The width of this interval can be upper bounded by the standard deviation of the λ-DF of the order pattern #0 since, according to Fig. 4.11, it is bigger than the average error in the estimation of $\phi_4(\lambda)$ for every value of λ . Therefore, the estimation of the control parameter comprises two stages:

1. An estimation of λ is performed by dividing the given Gray code, $\{g_i\}_{i=0}^{M-1}$, $g_i \in \{0,1\}$, into a large enough set of disjoint subsequences of length $N \gg 4$, say, $\{g_{k\cdot N+i}\}_{i=0}^{N-1}$ for $k = 0, 1, \ldots, K = \lfloor M - N \rfloor - 1$. For each such binary subsequence, a value of $\phi_4(\lambda)$ is then computed as the relative frequency of the order pattern $[0,1,2,3]$ using, of course, the Gray ordering (Sec. 3.3). Let $\bar{x}$ be the mean value of the resulting values of $\phi_4(\lambda)$. From $\phi_4(\lambda) = \lambda^2/(2-\lambda)$, Eq. (4.3), it follows that the control parameter is estimated as

$$\hat{\lambda} = \phi_4^{-1}(\bar{x}) = \frac{-\bar{x} + \sqrt{\bar{x}^2 + 8\bar{x}}}{2}. \tag{4.8}$$

2. If σ is the standard deviation of the $\phi_4(\lambda)$ sampling, then there exists a high probability that λ is in the interval

$$(\phi_4^{-1}(\bar{x} - \sigma), \phi_4^{-1}(\bar{x} + \sigma)). \tag{4.9}$$

The specifics of this procedure refers to the skew tent map, but the general strategy is the same, once a bijective λ-DF of an order pattern is exactly known.

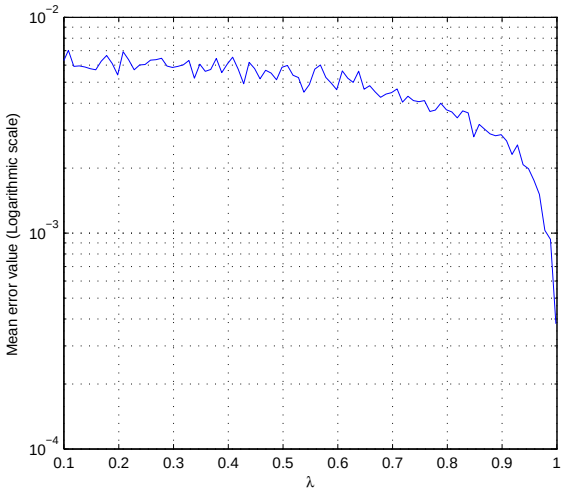


Figure 4.12: Mean error value in the estimation of the control parameter of the skew tent map.

In order to establish the accuracy of the procedure, some numerical simulations with the skew tent map were done. For every value of the control parameter, a group of 100 different initial conditions were used in the generation of the corresponding Gray codes. For each of these binary sequences, the control parameter λ was estimated as just explained. The mean error of the estimation is shown in Fig. 4.12. The average error lies always above 10^{-4}, and can only be reduced by the implementation of the procedure with extended-precision arithmetic libraries.

To prove this claim, the case of the symmetric tent map, i.e., the skew tent map for $\lambda = 1/2$, will be considered next. For the symmetric tent map the arithmetic is exact. Indeed, if $0.x_0x_1...x_M$, $x_i \in \{0, 1\}$, is the expansion to base 2 of $x \in [0, 1]$, i.e.,

$$x = \sum_{n=0}^{M} \frac{x_n}{2^{n+1}}, \tag{4.10}$$

(numbers with finite binary expansions are called dyadic rationals), then the action of the symmetric tent map amounts to a zero-bit dependent left shift, to wit:

$$f_{1/2}(0.x_0x_1...x_n...x_{M-1}x_M) = \begin{cases} 0.x_1x_2 \ldots x_{n+1} \ldots x_M 0, & \text{if } x_0 = 0 \\ 0.x_1^*x_2^* \ldots x_{n+1}^* \ldots x_M^* 0, & \text{if } x_0 = 1 \end{cases} \tag{4.11}$$

where $x_n^* = 1 - x_n$. Therefore, if $x \in [0, 1]$ is represented with M bits and $x_M = 1$, the orbit of x collapses to 0 after M iterations of $f_{1/2}$, so M can be considered the effective length of the orbits to be used in an estimation of $\lambda = 1/2$. For $\nu = 3$, the relative frequency of the order pattern #0 ($[0, 1, 2]$ in this case) was determined for a large set of random initial conditions x and increasing orbit lengths M. The convergence

in average of this relative frequency to $\phi_3(1/2) = 1/3$ (see Eq. (4.6)) as M increases, is confirmed by Fig. 4.13. At the same time, the variance of the estimation steadily reduces with M, as shown in Fig. 4.14. In other words, a higher precision of the arithmetic used in orbit generation and greater samples for the subsequent control parameter estimation, clearly improves the results. We conclude that the inaccuracies

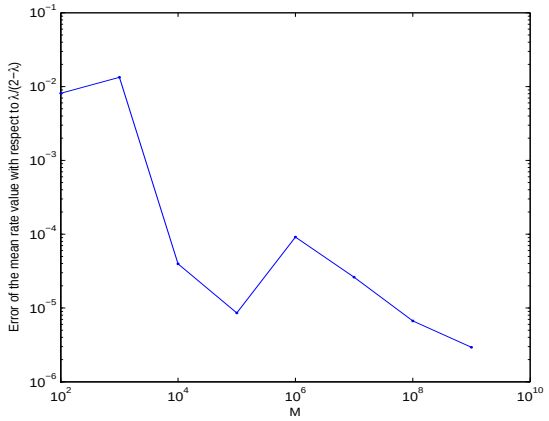


Figure 4.13: Dependency of the error in the estimation of the rate of occurrences of the order pattern #0 with respect to the length of the orbits.

exposed above in our method to recover the control parameter of maps of $\mathcal{F}_2$, based on the order patterns of their coarse-grained orbits (specifically, in form of Gray codes), are due to the shortcomings of finite precision arithmetic and finite statistical sampling, but are not inherent to the method —as proved with the symmetric tent map.

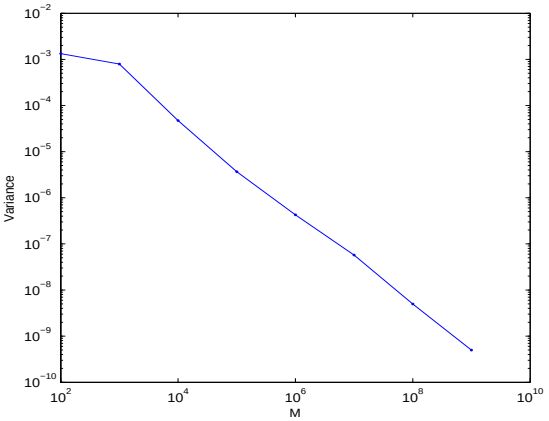


Figure 4.14: Variance of the error in the estimation of the rate of occurrences of the order pattern #0 with respect to the length of the orbits.

4.5 Concluding remarks

In this Chapter it was shown how to rebuild the λ-DFs of order patterns of unimodal maps from Gray codes, the scope being the estimation of the parameter λ. It has been analyzed the λ-DFs of the order patterns of two unimodal parametric maps: the logistic map (as representative of the subclass $\mathcal{F}_1$) and the skew tent map (as representative of the subclass $\mathcal{F}_2$). In the case of the logistic map, it turns out that this technique can hardly deliver, on account of the complex and many-to-one relation between λ and those λ-DFs. On the contrary, this relationship is simple, one-to-one, and analytically known for $\pi = [0, 1, ..., \nu - 1]$ in the case of the skew tent map. The method described improves previous proposals for parameter estimation from symbolic sequences of unimodal maps in that a knowledge of the critical point value is not needed. The most important consequence of this Chapter is that symbolic sequences of unimodal maps cannot be used as keystreams of stream ciphers. Indeed, the work described in [Wu04] along with our method, pinpoints a critical vulnerability in encryption systems such as the one introduced in [Kurian08]. However, the method demands high computational precision and large amounts of data. In this regard, it is advisable the use of extended-precision libraries for good estimations. In the ideal case of arbitrarily high precision, the estimated value of the control parameter is arbitrarily close to the real one.

Chapter 5

Design rules: lessons learned from the cryptanalysis of digital chaos-based cryptosystems

5.1 Introduction

The core of digital chaos-based cryptography is the selection of a *good* chaotic map for a given encryption scheme. Actually, the presence of chaos does not guarantee the security of an encryption algorithm [Kocarev01a]. A good digital cryptosystem based on chaos should not be just the concomitance of a chaotic map and an encryption architecture, but the result of their *synergical* association. Indeed, the quality of a chaotic map for cryptography must be evaluated not just with considerations on its dynamic properties, but also with considerations on the needs of the sustaining encryption architecture. In other words, from a general point of view it is not possible to design chaotic cryptosystems satisfying the *chaotic-system-free property* [Li03, p. 30] and, as a result, the selection of a certain encryption scheme demands the selection of a group of chaotic maps satisfying a certain set of dynamical properties. Finally, digital chaos-based cryptography is implemented on computers and thus the problem derived from finite-precision computation must be evaluated and conveniently handled during the design stage. This Chapter illustrates the problems with three elements involved in the design of digital chaos-based cryptosystems, i.e., the selection of a chaotic map (Sec. 5.2), the selection of an encryption architecture (Sec. 5.3) and the implementation of the encryption system (Sec. 5.4). Although it is impossible to guarantee the total security of a cryptosystem, in Sec. 5.5 a minimum set of rules is established to avoid the problems explained in this Chapter. Finally, in Sec. 5.6 the adequacy of the set of rules is illustrated by evaluating some recent proposals in the field of digital chaos-based cryptography.

5.2 Problems with the selection of the chaotic system

Problem 1. ***Definition of the key leading to non-chaotic behavior.*** *In some chaos-based cryptosystems the control parameters of the underlying chaotic systems are determined by the secret key. If the link between the secret key and the control parameters is not established carefully, then it is possible that the underlying chaotic system evolves in an non-chaotic way, which further erodes the confusion and diffusion properties required by the resulting cryptosystem.*

The chaotic systems used as base of cryptosystems are defined in a parametric way such that their dynamics depends on one or several control parameters. Moreover, those chaotic systems are dynamical systems which show a chaotic behavior 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 the set of values for the control parameters leading to chaos. Otherwise, the underlying dynamical system associated to the cryptosystem (or encryption system) evolves non-chaotically, which implies the reduction of the level of entropy in the ciphertext (i.e., the output of the cryptosystem) and of the influence on the ciphertext of a change in the plaintext (i.e., the input of the cryptosystem). This problem is specially relevant when the design of the cryptosystem is based on a dynamical system with chaotic behavior only for a set of disjoint intervals of values of the control parameters. This is the case of the logistic map and the Hénon map, which have been used in [Pisarchik06; Ling07; Wang08c] and in [Chee06] respectively without a thoroughly analysis of their dynamics, as we have pinpointed in [Arroyo08d; Arroyo09g; Arroyo09f; Arroyo08b]. As a conclusion, it is highly advisable to use dynamical systems with chaotic behavior for all the values of the control parameter(s). That is, *robust chaotic systems* [Banerjee98] should be used instead of nonrobust ones.

Problem 2. ***Nonuniform probability distribution function.*** *In some chaos-based encryption architectures the confusion and/or diffusion properties depend on the probability distribution function of the orbits derived from the selected chaotic systems. If that distribution is not uniform and independent of the values of control parameters, then the quality of the diffusion process is reduced.*

The iteration of a chaotic map can be used to generate pseudo-random sequences to encrypt the plaintext. The encryption procedure could be performed by different ways, but all of them demand the equiprobability of all the states contained in the

pseudo-random sequences. If this requirement is not satisfied, then the conditional entropy of the ciphertext with respect to the plaintext may be large enough to leak information about relationships between the output and the input of the target cryptosystem (see the entropy attack in [Alvarez03b]). This effect is specially significant for image encryption, as pointed out recently by [Li07a]. As a remedy, chaotic maps with a uniform probability distribution function should be selected as base of this kind of cryptosystems, being the family of piecewise linear chaotic maps [Li05b] a good option.

Problem 3. ***Return map reconstruction.*** *The ciphertext of some cryptosystems makes it possible to reconstruct a return map of the underlying chaotic system. If such a return map is meaningful, then an attacker may be able to infer the values of the control parameters that govern the evolution of the chaotic system.*

The most direct way to estimate the control parameters from a chaotic orbit is to plot x_{n+1} versus x_n, which is actually the chaotic map itself. If this representation shows a simple function between x_{n+1} and x_n, then it could be possible to infer the control parameter. In [Skrobek08] a chosen-ciphertext attack is used to build a discretized version of the logistic map which further leads to the estimation of the control parameter. One solution against this kind of attack is to shuffle/truncate the chaotic orbit before using it for encryption, which randomizes the plot of the return map.

Problem 4. ***Degradation of the efficiency of digital chaos-based cryptosystems based on continuous-time chaotic systems.*** *In digital chaos-based cryptography the encryption procedure is performed in discrete time. Therefore, if the underlying chaotic system is defined in continuous time, then it is necessary to apply some numerical method to obtain the chaotic orbits. The application of these numerical methods increases the time to compute the orbits, and thus the encryption time.*

The structural complexity of a chaotic system is a critical element when evaluating its suitability for cryptographic applications. With this bottom line in Sec. 1.3.3 we emphasized that structural complexity can be minimized by selecting chaotic systems defined in discrete time. Indeed, in discrete time chaos can be achieved for phase space of dimension 1, whereas it has to be at least of dimension 3 when considering continuous time. Furthermore, the rule of evolution of continuous-time chaotic systems requires to solve a system of differential equations [Hirsch74, p. 160]. From a general point of view, the solution of those differential equations cannot be accomplished analytically, and thus numerical methods must be applied. Numerical

methods for the resolution of differential equations are high time consuming. As a result, for a given encryption architecture with underlying chaotic system defined in continuous-time, the encryption time is greater than the encryption time obtained when the chosen dynamical system is a chaotic map. For the sake of argument, let us consider our cryptanalytical work [Arroyo09h] on the chaos-based cryptosystem proposed in [Gao08a]. These cryptosystems are intended to encrypt images through the concatenation of a shuffling and masking procedures. The shuffling procedure is based on the iteration of the logistic map, whereas masking is built upon the iteration of two continuous-time chaotic systems: Lorenz' [Lorenz63] and Chen's systems [Chen99]. The Lorenz system is given by

$$\begin{aligned} \frac{dx_1}{dt} &= \alpha x_1 + \alpha x_2, \\ \frac{dx_2}{dt} &= -x_1 x_3 + \beta x_1 - x_2, \\ \frac{dx_3}{dt} &= x_1 x_2 - \rho x_3, \end{aligned} \tag{5.1}$$

where α, β, and ρ are control parameters. The Lorenz system is chaotic for $\alpha = 10$, $\beta = 28$, and $\rho = 8/3$. On the other hand, the Chen system is defined as

$$\begin{aligned} \frac{dx_1}{dt} &= \eta(x_2 - x_1), \\ \frac{dx_2}{dt} &= (\sigma - \eta)x_1 - x_1 x_3 + \sigma x_2, \\ \frac{dx_3}{dt} &= x_1 x_2 - \delta x_3, \end{aligned} \tag{5.2}$$

being chaotic for $\eta = 35$, $\sigma = 28$, and $\delta = 3$. Because the chaotic iterations of Lorenz' and Chen's systems involve complicated numerical differential functions, the encryption speed is expected to be very slow compared with other traditional ciphers. To asses this fact, we derived a modified encryption scheme from the original one by replacing the Lorenz and Chen systems with the logistic map, and then compared the encryption speeds of the two cryptosystems. Both cryptosystems were implemented using MATLAB on a PC with a 1.6 GHz processor and 512 MB of RAM. For images of size 256×256, the typical encryption time for the original cryptosystem in [Gao08a] was around 5.8 s, while the modified cryptosystem based on the logistic map required on average around 1.2 s to encrypt an image. The experiments have clearly shown that using continuous chaotic systems can drastically reduce the encryption speed. Since there are also no other obvious merits in using continuous chaotic systems rather than a simple discrete-time chaotic map, the use of Lorenz' and Chen' systems in the image encryption scheme under study is unnecessary. Instead, these continuous-time chaotic

systems can be replaced by a simpler discrete-time chaotic map without compromising the security. This statement is a general rule when designing encryption procedures working in discrete time.

Problem 5. ***Part of the key should not leak the rest of the key.*** *In some cryptosystems the secret key is composed of different subkeys. If the knowledge of some subkeys allow the recovery of the rest of the key, then a* partial key recovery attack *can be performed. Therefore, the design of a cryptosystem must guarantee that the different subkeys composing the secret key are uncorrelated.*

In the context of a secure and robust encryption system it is assumed that the partial knowledge of the key does not reveal information about the rest of the key and, as a result, the cryptosystem performance is not harmed [Alvarez06b, Rule 7]. However, in the scenario drawn by [Chee06], partial knowledge of the key can be used to obtain the rest of the key (Case study 2.2.1). Next we show how a known-plaintext attack can be employed to reconstruct Eq. (2.12), Eq. (2.13), and v_0 (initial condition of the underlying Hénon map defined in Eq. (2.7)) when Eq. (2.11) is known. Given two plaintexts $\{p_{1,k}\}_{k=0}^{N-1}$, $\{p_{2,k}\}_{k=0}^{N-1}$, then

$$u_{1,1} = 1 - \psi(p_{1,0}) \cdot \mu_1(v_0) \cdot u_0^2 + v_0, \tag{5.3}$$
$$u_{2,1} = 1 - \psi(p_{2,0}) \cdot \mu_1(v_0) \cdot u_0^2 + v_0, \tag{5.4}$$

and

$$u_{1,k+1} = 1 - \psi(p_{1,k}) \cdot \mu_1(v_k) \cdot u_{1,k}^2 + v_k, \tag{5.5}$$
$$u_{2,k+1} = 1 - \psi(p_{2,k}) \cdot \mu_1(v_k) \cdot u_{2,k}^2 + v_k, \tag{5.6}$$
$$v_k = \mu_2(v_{k-1}) \cdot u_{k-1}, \tag{5.7}$$

where $k \geq 1$. Subtracting Eq. (5.3) from Eq. (5.4), one obtains:

$$\begin{aligned} u_{2,1} - u_{1,1} &= \psi(p_{1,0}) \cdot \mu_1(v_0) \cdot u_0^2 - \psi(p_{2,0}) \cdot \mu_1(v_0) \cdot u_0^2 \\ &= (\psi(p_{1,0}) - \psi(p_{2,0})) \cdot \mu_1(v_0) \cdot u_0^2. \end{aligned} \tag{5.8}$$

In the following discussion, it is shown how to recover the secret key, assuming that $\psi(x)$ is known.

From Eq. (5.8), one has

$$r_1 = \frac{u_{2,1} - u_{1,1}}{\psi(p_{1,0}) - \psi(p_{2,0})}. \tag{5.9}$$

Because the encryption is generally carried out in floating point operation, the quantization error is very small is most cases so it can just be ignored. As a result, $r_1 = \mu_1(v_0) \cdot u_0^2$, which implies that $v_0 = u_{1,1} - 1 + \psi(p_{1,0}) \cdot r_1$, and $\mu_1(v_0) = \frac{r_1}{u_0^2}$.

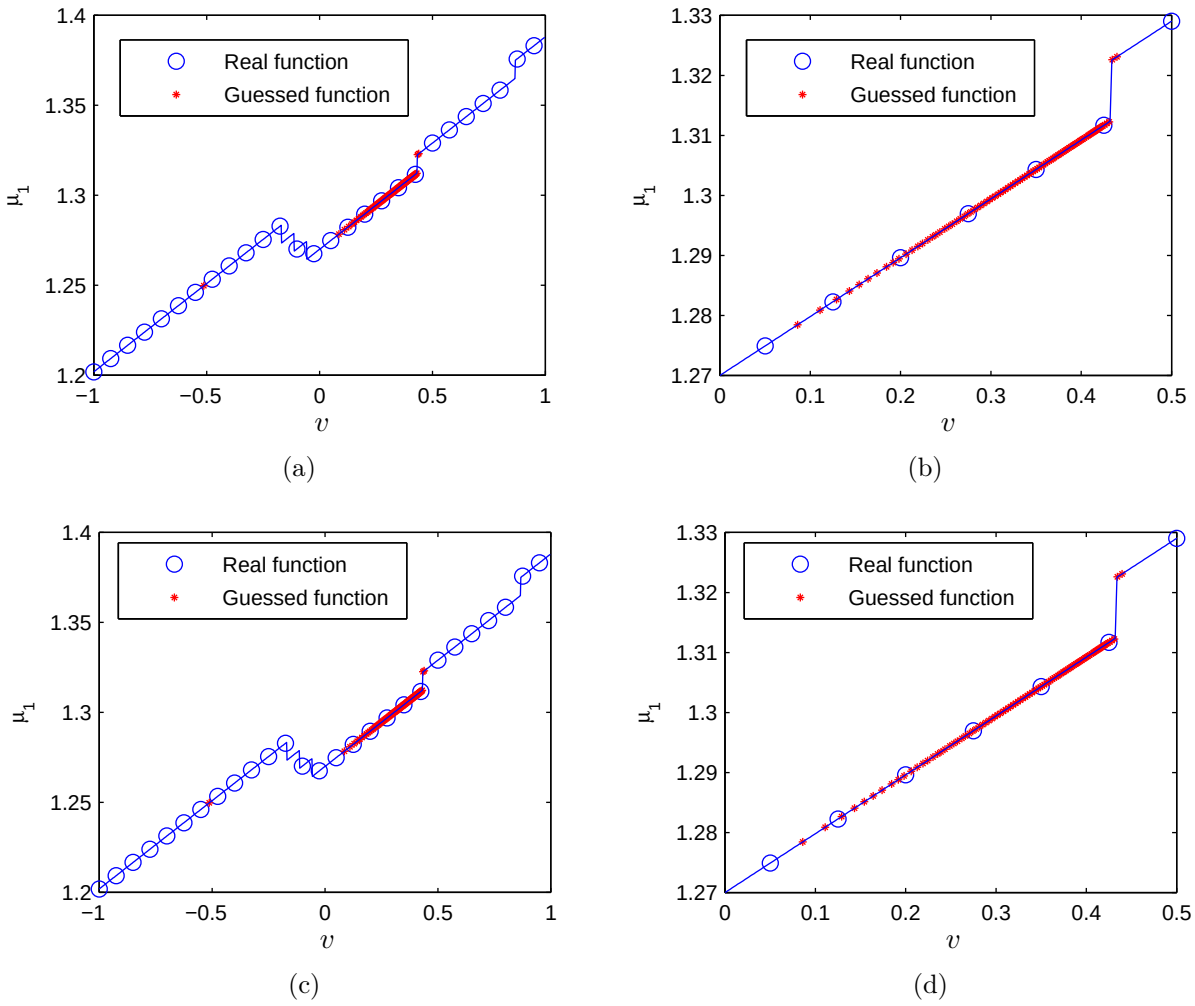


Figure 5.1: Recovered and original functions for the PRSK mechanism when they are designed as in [Chee06] (a) $\mu_1(v)$ for $v_0 = 0.9402036$; (b) image zoom for $\mu_1(v)$ and $v_0 = 0.9402036$; (c) $\mu_1(v)$ for $v_0 = -0.5123493$; and (d) image zoom for $\mu_1(v)$ and $v_0 = -0.5123493$.

Subtracting Eq. (5.5) from Eq. (5.6):

$$\widetilde{\mu}_1(v_k) = \frac{u_{2,k+1} - u_{1,k+1}}{\psi(p_{1,k}) \cdot u_{1,k}^2 - \psi(p_{2,k}) \cdot u_{2,k}^2}. \tag{5.10}$$

From Eq. (5.7):

$$\widetilde{\mu}_2(v_{k-1}) = \frac{u_{1,k+1} - 1 + \psi(p_{1,k}) \cdot \widetilde{\mu}_1(v_k) \cdot u_{1,k}^2}{u_{k-1}}. \tag{5.11}$$

As mentioned above, by ignoring the quantization error, we have $\widetilde{\mu}_1(v_k) = \mu_1(v_k)$ and $\widetilde{\mu}_2(v_{k-1}) = \mu_2(v_{k-1})$.

It is possible to reconstruct $\mu_1(v_k)$ and $\mu_2(v_k)$ repeating this procedure for $k = 1, \ldots, N$.

In order to prove the proposed known-plaintext attack, 10000 points for $\mu_1(v_k)$ and $\mu_2(v_k)$ were calculated for $u_0 = 0.4,\ v_0 = 0.9402036$ and $u_0 = 0.4,\ v_0 = -0.5123493$. In Fig. 5.1 and Fig. 5.2 it is shown how it was possible to infer $\mu_1(v_k)$, $\mu_2(v_k)$ shape. This is due to the fact that the first component of the Hénon map employed in the encryption process is sent through the communication channel without applying any masking transformation. However, there exists an underlying quantization error in the recovering method due to the fact that all the mathematical operations are done in finite precision. It was verified that $\Delta(\mu_1) = |\widetilde{\mu}_1 - \mu_1| \sim 10^{-6}$ and $\Delta(\mu_2) = |\widetilde{\mu}_2 - \mu_2| \sim 10^{-7}$. Therefore, the exact μ_1 and μ_2 reconstruction demands an exhaustive search. On the other hand, Fig. 5.1 and Fig. 5.2 also show that during the encryption process $\mu_1(v_k)$ and $\mu_2(v_k)$ do not go through all the possible values of the functions referred by Eqs. (2.12) and (2.13). In other words, it was verified that, during the encryption process, v_k never goes through all the possible input values for both functions. This is the reason why $\mu_1(v)$ and $\mu_2(v)$ can not be totally recovered, which has no impact on the efficiency of the cryptanalysis.

5.3 Problems with the encryption architecture

Problem 6. ***Bad definition of the ciphertexts.*** *A bad definition of the ciphertext derived from a chaos-based cryptosystem could allow the estimation of the initial condition(s) and/or the control parameter(s) of the underlying chaotic system. This problem is present in some chaos-based cryptosystems whose ciphertext is given by fragments of orbits, sampled versions of the orbits, or discretized versions of the orbits of the underlying chaotic systems.*

A m-dimensional discrete-time chaotic map is defined by the rule of evolution

$$x_{n+1} = f_\lambda(x_n),$$

and, as a result, the ciphertext can not be the orbits of the map since it may allow the estimation of λ from $m+1$ or a bit more consecutive units of ciphertext. This is the case of the cryptosystem proposed in [Ling07], and which we have cryptanalyzed in [Arroyo09g].

Case study 5.3.1 ([Arroyo09g])**.** *Cryptanalysis of the cryptosystem described in [Ling07]*

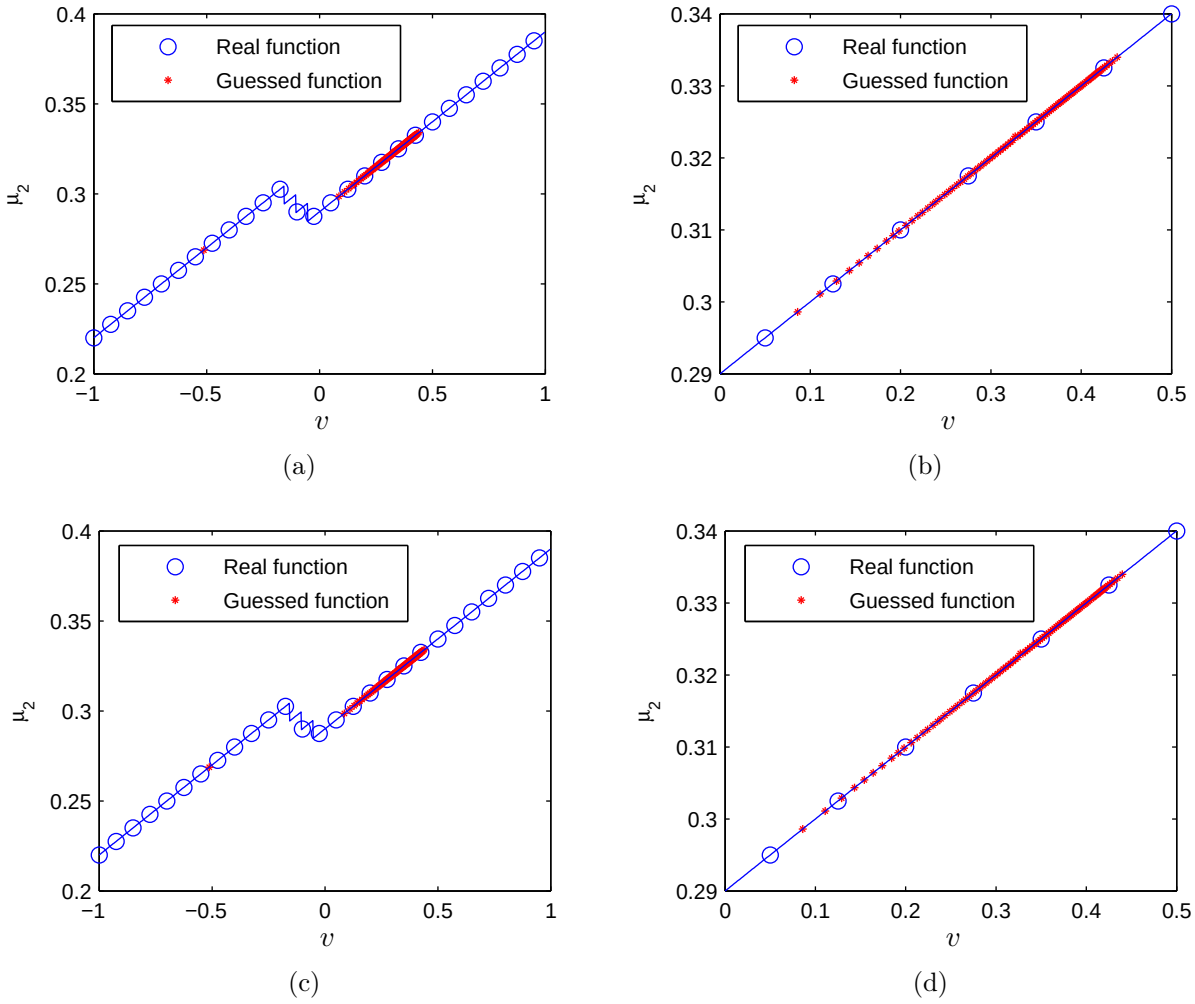


Figure 5.2: Recovered and original functions for the PRSK mechanism when they are designed as in [Chee06] (a) $\mu_2(v)$ for $v_0 = 0.9402036$; (b) image zoom for $\mu_2(v)$ and $v_0 = 0.9402036$; (c) $\mu_2(v)$ for $v_0 = -0.5123493$; and (d) image zoom for $\mu_2(v)$ and $v_0 = -0.5123493$.

In [Ling07] the encryption procedure is carried out by decomposing the input plaintext signal into two different subbands and masking each of them with a pseudo-random number sequence generated by iterating the chaotic logistic map. The decomposition of the input plaintext signal x_n is driven by

$$t_n = K \sum_{\forall j} x_j h_{2n-j}, \tag{5.12}$$

$$t'_n = K' \sum_{\forall j} x_j h'_{2n-j}. \tag{5.13}$$

Then, the masking stage generates the ciphertext signal (v_n, v'_n) according to the

following equations:

$$v_n = t_n + \alpha(t'_n), \tag{5.14}$$

$$v'_n = t'_n - \alpha'(v_n), \tag{5.15}$$

where $\alpha(u) = u + s_n$ ($\alpha'(u) = u + s'_n$) and s_n (s'_n) is the state variable of the logistic map (Eq. (1.9)).

The secret key of the cryptosystem is composed of the initial conditions and the control parameters of the two logistic maps involved, i.e., s_0, s'_1, λ and λ'.

In a known-plaintext attack the cryptanalyst possesses a plaintext signal $\{x_n\}$ and its corresponding encrypted subband signals $\{v_n\}$ and $\{v'_n\}$. Because $\{h_n\}$, $\{h'_n\}$, K and K' are public, we can get $\{t_n\}$ and $\{t'_n\}$ from $\{x_n\}$. Then we can get the values of $\{s_n\}$ and $\{s'_n\}$ as follows:

$$s_n = v_n - t_n - t'_n, \tag{5.16}$$

$$s'_n = t'_n - v_n - v'_n. \tag{5.17}$$

For $n = 0$, the values of the subkeys s_0 and s'_0 have been obtained. Furthermore, we can obtain the control parameters by just doing the following operations:

$$\lambda = \frac{s_{n+1}}{s_n(1 - s_n)},$$

$$\lambda' = \frac{s'_{n+1}}{s'_n(1 - s'_n)}.$$

Consequently, the orbits of chaotic maps cannot be employed directly as keystreams. Furthermore, if the invariant set of the chaotic map has a size dependent on the control parameters, even sampled versions of the orbits may allow the estimation of the control parameters through a ciphertext-only attack. As explained in Sec. 2.3 (Case study 2.3.1), we have analyzed this situation in [Arroyo08d], being the case study the cryptosystem defined in [Pisarchik06]. Finally, the theory of symbolic dynamics could reveal the weakness of a cryptosystem if the ciphertext allows to get the symbolic sequences of a chaotic map. In Sec. 3.5 (Case study 3.5.1) we have shown through a chosen-ciphertext attack how to derive the symbolic sequence of the logistic map driving the encryption procedure defined in [Wang08c]; once we have the symbolic sequence, we can infer the values of the control parameter and initial condition of the underlying logistic map according to the theory of applied symbolic dynamics described in Chapter 3.

Problem 7. ***Efficiency of the cryptosystem depending on the value of the key.*** *If the encryption and decryption times depend on the key or a subkey, then a timing attack can be performed to estimate the (sub)key.*

Some encryption architectures perform the transformation of the plaintext into the ciphertext through several encryption rounds. Additionally, in each encryption round a chaotic map is iterated n times. Since the encryption and decryption times have to be constant and independent of the value of the key, it is not a good practice to select the number of encryption rounds and n as part of the key. Otherwise, a timing attack [Kocher96; Brumley03] based on the analysis of the encryption and decryption time can be used for the partial estimation of the secret key, which is a serious security flaw. Let us exemplified a timing attack by recalling the cryptosystem proposed in [Pisarchik06]. As it has been shown in Sec. 2.3, in every encryption round of the cryptosystem under consideration, Step 3 is carried out through the n iterations of Eq. (1.9), where n is a subkey. This means that, for a certain number of encryption rounds (i.e., a certain value of j) and a certain value of the control parameter λ, the encryption speed decreases as n increases. Similarly, because the encryption/decryption procedure is composed of j repeated cycles, the encryption speed will also become slower if the value of j increases. To be more precise, for a given plain-image, we can expect the existence of the following bi-linear relationship between the encryption/decryption time (EDT) and the values of n and j:

$$EDT(n, j) \approx (c \times n + d_0) \times j + d_1, \tag{5.18}$$

where c corresponds to the common operations consumed on each chaotic iteration, d_0 to the operations performed in each cycle excluding those about chaotic iterations, and d_1 to those operations performed on the initialization process and the postprocessing after all the j cycles are completed. In addition, because λ is just the control parameter of the chaotic map, it is expected that EDT will be independent of its value.

With the aim of verifying this hypothesis, some experiments have been made under the following scenario. An image with random pixel values of size 256×256 was encrypted for different values of λ, n and j. The encryption time corresponding to each key is shown in Fig. 5.3, from which one can see that Eq. (5.18) is verified.

The above experimental results ensure the feasibility of a timing attack to a subkey of the cryptosystem under study: by observing the encryption time, it is possible to estimate the value of n if j is known and vice versa. Without loss of generality, assuming an attacker Eve knows the value of n, but not that of j, let us demonstrate how the timing attack can be performed in practice. In this case, the relationship between EDT and the value of j can be simplified as $EDT(n, j) = c_n \times j + d_n$, where $c_n = c \times n$ and $d_n = d_0 \times j + d_1$. Then, if Eve gets a temporary access to the encryption (or decryption) machine, she can carry out a real timing attack in the following steps:

1. She observes the whole process of encryption (or decryption) to get the encryption (or decryption) time t_j and also the size of the ciphertext (i.e., the size of the plaintext).

2. By choosing two keys with different values of j, she encrypts[1] a plaintext (or decrypts a ciphertext) of the same size and gets t_1 and t_2.

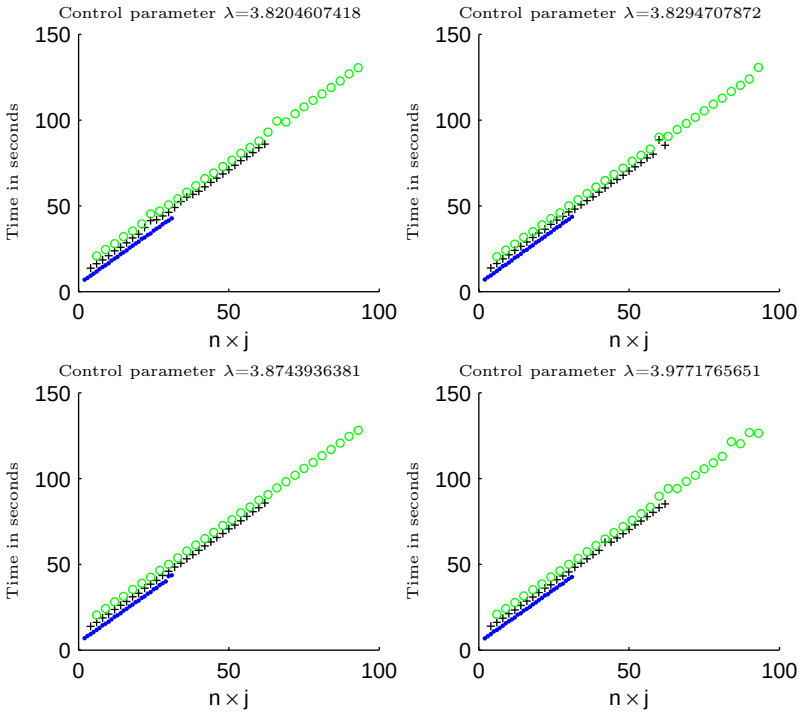


Figure 5.3: Encryption time for images of size 256×256 and different values of the number of iterations n and the number of encryption rounds.

3. She derives the values of c_n and d_n by substituting t_1 and t_2 into $EDT(n, j) = c_n \times j + d_n$.

4. She estimates the value of j to be $\hat{j} = \text{round}((t_j - d_n)/c_n)$.

5. She verifies the estimated value $\hat{j}$ by using it to decrypt the observed ciphertext. If the recovered plaintext is something meaningful, the attack stops; otherwise, she turns to search the correct value of j in a small neighborhood of $\hat{j}$ until a meaningful plaintext is obtained.

[1]Please note that this can be done on her own computer, as long as she has the encryption/decryption software installed.

As a result of the previous analysis, the number of encryption rounds and the number of iterations of the map should be public parameters of the chaos-based cryptosystem instead of part of the key.

Problem 8. ***Faulty derivation of the parameters of the chaotic system from the key.*** *In some chaos-based cryptosystems the key is used to derive the values of the parameters necessary to iterate a chaotic system and finally encrypt the information. If this mapping implies a reduction of the key space, i.e., that it is only used a subset of the possible values of those parameters, then a brute-force attack on the values of the parameter could be much less demanding than the one on the secret key.*

One important step in the design of a chaos-based cryptosystem is to decide what the key is. One possibility is to use the control parameters and the initial conditions of the underlying chaotic systems as the secret key or as part of the secret key. Another option is to establish the values of the control parameters and the initial conditions of the maps from the secret key through a certain function. In this sense, it must be assured that the image set of that function is the whole set of possible values of the control parameters and the initial conditions. Otherwise, a brute-force attack can be performed on the reduced space of control parameters and initial condition values with a lower computational cost than the one on the key space. A cryptosystem with this problem was introduced in [Pareek03] and was later cryptanalyzed in [Alvarez03a].

Problem 9. ***Encryption procedure equivalent to a map only dependent on the key.*** *If the transformation of the plaintext into the ciphertext is determined by a procedure equivalent to a map only dependent on the key, then known/chosen-plaintext attacks may be performed to reconstruct the transformation procedure.*

In some encryption schemes the transformation of the plaintext into the ciphertext is led either by a procedure derived using only the key, or by a sampling process on a sequence of values generated using only the key. In those situations, it could be possible to estimate either the key or to make up some function somehow equivalent to the encryption procedure. For example, if the encryption procedure consists of searching plaintexts in pseudo-random sequences generated by iterating a chaotic map, since the pseudo-random sequence remains unchanged unless the key is modified, then it is possible to reconstruct the pseudo-random sequence through a chosen-plaintext attack (see [Alvarez04f; Alvarez04g]). This problem also exists in those schemes where the encryption procedure consists of a permutation-only stage which is fixed unless the control parameters and initial conditions change, i.e., unless the the secret key is updated. In order to clarify this matter, let us consider again the cryptosystem defined in [Gao08a].

Case study 5.3.2 ([Arroyo09h]). *Cryptanalysis of the cryptosystem defined in [Gao08a]*

As mentioned above, the cryptosystem under consideration consists of two stages: a shuffling stage and a masking stage. Assuming that the size of the plain-image $\mathbf{I}$ is $M \times N$ and the cipher-image is $\mathbf{I}'$, the encryption scheme proposed in [Gao08a] can be described by the following two procedures.

- *Shuffling procedure*

  In this procedure, the plain-image $\mathbf{I}$ is permuted to form an intermediate image $\mathbf{I}^*$ according to a total shuffling matrix $\mathbf{P}^*$, which is derived by pseudo-randomly permuting the rows and columns of the original position matrix $\mathbf{P} = [(i, j)]$. The pseudo-random row and column permutations are generated by iterating the logistic map (Eq. 1.9) with $\lambda = 4$ from a given initial condition x_0.

- *Masking procedure*

  In this procedure, the intermediate image $\mathbf{I}^*$ is further masked by a keystream $\{B(i)\}_{i=1}^{MN}$ as follows: $\forall i = 1 \sim MN$, $I'(i) = I^*(i) \oplus B(i) \oplus I'(i-1)$, where $I(i)$, $I'(i)$ denote the i-th pixels of $\mathbf{I}^*$ and $\mathbf{I}'$ (counted from left to right and from top to bottom), respectively, and $I'(0) = 128$.

The keystream $\{B(i)\}_{i=1}^{MN}$ is generated by iterating Lorenz' [Lorenz63] and Chen's [Chen99] systems and doing some postprocessing on all the variables of state. When a variation of stream cipher is created, as in the case under study, obtaining the keystream is totally equivalent to obtaining the key whenever different plain-images are encrypted using the same key. Upon this hint, in [Arroyo09h] we have carried out a chosen-plaintext attack to recover both the keystream and the shuffling matrix of the cryptosystem described in [Gao08a]. Let us choose a plain-image $\mathbf{I}_1$ such that $\forall i, j = 1 \sim MN$, $I_1(i) = I_1(j) = \theta$. In this case, the shuffling part does not work, so we have $\mathbf{I}_1^* = \mathbf{I}_1$. Then, we can recover the keystream as follows: $\forall i = 1 \sim MN$, $B(i) = I_1(i) \oplus I_1'(i) \oplus I_1'(i-1)$. After removing the masking part, we can try to recover the shuffling matrix. According to the general cryptanalysis on permutation-only ciphers in [Li08], only $\lceil \log_{256}(MN) \rceil$ chosen plain-images are needed to recover the shuffling matrix $\mathbf{P}^*$. In total we need $\lceil \log_{256}(MN) \rceil + 1$ chosen plain-images to perform this chosen-plaintext attack.

As a conclusion, the encryption function that transforms a unit of plaintext into a unit of ciphertext should depend on the key and on the whole plaintext.

(a)

(b)

(c)

Figure 5.4: Illustration of the low sensitivity to the change of the plain-image: (a) the first plain-image $\mathbf{I}_0$; (b) the second plain-image $\mathbf{I}_1$ (only the center pixel is different from $\mathbf{I}_0$); (c) the differential cipher-image $\mathbf{I}'_0 \oplus \mathbf{I}'_1$.

Problem 10. ***Low sensitivity to the change of plaintext.*** *In some encryption architectures plaintexts with slightest differences are associated to very similar ciphertexts, which is a clear violation of the diffusion property.*

This problem is specially relevant when considering the encryption of images. This being the case, the encryption scheme must guarantee that two images differing in just one pixel determine two totally different cipher-images. This requirement is not satisfied if encryption is performed through just one encryption round, as it occurs with the cryptosystem proposed in [Gao08a] (Case study 5.3.2). For that cryptosystem, given two plain-images $\mathbf{I}_0$ and $\mathbf{I}_1$ with only one pixel difference at the position (i, j), the difference will be permuted to a new position (i^*, j^*) according to

the shuffling matrix $\mathbf{P}^*$. Then, because all plain-pixels before (i^*, j^*) are identical for the two plain-images, the ciphertexts will also be identical. This shows the low sensitivity of the image encryption scheme to changes in the plain-image. Figure 5.4 gives an example of this problem. It can be seen how the differential cipher-image is equal to zero for any pixel before (i^*, j^*) and equal to a constant value after that position.

5.4 Implementation problems

Problem 11. ***Non-invertible encryption procedure.*** *The iteration of the chaotic systems sustaining chaos-based cryptosystems implies working with real numbers. Since the implementation of chaos-based cryptosystems is done with finite precision arithmetic, round-off operations could lead to a non-invertible encryption procedure.*

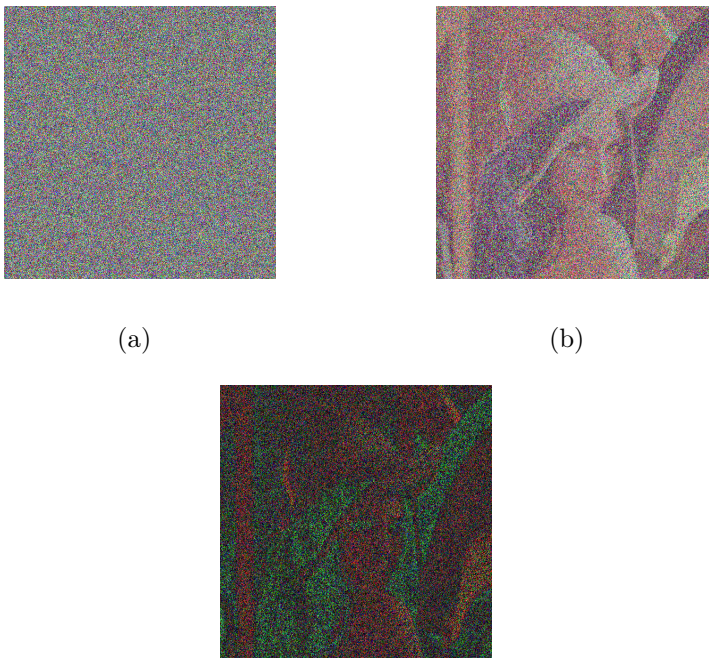
One critical point when working with dynamical systems and the analysis of their dynamics is the selection of a right simulation framework. Indeed, the computer-based analysis of dynamical systems could lead to some conclusions different from those expected from theory. This divergence also influences and conditions chaos-based cryptosystems. Thus, if the characteristics and problems of finite-precision are not handled properly, then it is possible that the orbits generated as base of encryption procedure can not be regenerated exactly during the decryption stage and, consequently, the original plaintext can not be recovered even when the key is known. This problem is not only relevant for fixed-point arithmetic but also for floating-point one. Indeed, the round-off quantization errors could lead to the occurrence of a non-invertible function for encryption and, as a result, the decryption process will be impossible. The cryptosystems introduced in [Pisarchik06; Chee06] are examples of the consequences of not handling conveniently the limitations of finite precision arithmetics, as we have pinpointed in [Arroyo08d; Arroyo08b]. To clarify the problem under consideration, let us recall the scope depicted in [Pisarchik06], whose goal is to encrypt images (Case study 2.3.1). The cryptosystem described in [Pisarchik06] generates a ciphertext consisting of a number of real values. Encryption is performed through j encryption rounds, being $\{x_c^i(r)\}_{i=1}^J$ ($c =$ R, G and B, $r \in \{1, 2, \ldots, j-1\}$) the output in the r-th encryption round corresponding to color component c of the i-th pixel of the image of length $J = M \times N$. All the operations to encrypt an image in [Pisarchik06] are performed using floating-point arithmetic. From Sec. 2.3 we know that $x_c^i(r) = x_n + x_c^i(r-1)$, where x_n is the resulting value of iterating the logistic map n times from x_0, according to Eq. (2.1) and Eq. (1.9). Hence, if during the decryption process we want to recover $x_c^i(r-1)$ (the original value of the i-th element in the

last round), we have to iterate n times the logistic map from x_0 to get x_n and, after that, to substract this value from $x_c^i(r)$. However, the resulting value of this previous operation might not match the actual value of $x_c^i(r-1)$, due to the *wobbling precision problem* that exists when dealing with floating-point operations [Higham61, p. 39]. This wobbling precision problem also causes the resulting guessed value of $x_c^i(r-1)$ to depend on the cryptosystem implementation. Therefore, if an image is encrypted on one platform and decrypted on another, and the implementations of floating-point arithmetics on both platforms are not compatible with each other, then the decrypted image might not match the original one. In [Pisarchik06] the cryptosystem was implemented using Microsoft Visual C# .NET 2005 and no comment was given about the wobbling precision problem in the decryption process. However, we have experimentally verified that this problem indeed exists when the cryptosystem is implemented using MATLAB on a PC with a 3 GHz processor and 2 GB of RAM. A very useful measure of the performance of the decryption procedure is the Mean Square Error or MSE. For P and P' being a plain image and the decrypted image respectively, the MSE for the color component c is defined as

$$MSE_c = \sum_{i=1}^{m} (P_c^i - P'^i_c)^2 / J, \tag{5.19}$$

where $c \in \{R, G, B\}$, $J = M \times N$ is the number of pixels of the images considered and the sequences $\{P_c^i\}_{i=1}^J$ and $\{P'_c\}_{i=1}^J$ are the result of scanning P and P' in the raster order. Consequently, for a well designed encryption/decryption scheme the MSE should be 0 for each color component. Unfortunately, for the cryptosystem under study, the values of MSE for all three color components are generally not equal to 0 due to the wobbling precision problem associated to the floating-point arithmetic. In order to evaluate the underlying decryption error of the cryptosystem defined in [Pisarchik06], a 512×512 plain-image "Lena", as shown in Fig. 2.8, was encrypted and decrypted using the same key $(n, j, \lambda) = (30, 1, 3.9)$. The results showed that the three MSEs obtained for the red, green and blue components of the decrypted image with respect to the original one were 6.49, 0.018, 0.057, respectively. For another key $(n, j, \lambda) = (30, 3, 3.9)$, the obtained MSEs were 206.96, 123.45, 58.65, respectively. Figure 5.5 shows the decrypted image and the error image when the cryptosystem was implemented in MATLAB using a third key $(n, j, \lambda) = (5, 2, 3.9)$.

Problem 12. ***Dynamical degradation.*** *The implementation of chaotic systems in finite precision in digital computers leads often to dynamical properties completely different from the theoretical and expected ones. If this deviation is not considered*



(a) (b)

(c)

Figure 5.5: Simulations with MATLAB (a) Ciphertext of the plain-image "Lena" (visualized as a pseudo-image by using Eq. (2.18)) (b) Recovered image of "Lena" using the same key (c) The error image between the original and the recovered "Lena".

during the design of chaos-based cryptosystems, it could imply a reduction of the performance and even a compromise of the security of the resulting cryptosystem.

This problem is closely related to the previous one, although the point of interest moves to degradation of dynamical properties of the implemented chaotic system with respect to the theoretical model. Consequently, the design of an encryption scheme using a chaotic system must be done by considering its practical implementation (not only the theoretical model). In [Alvarez06a] some consequences of the dynamical degradation of a chaotic map are shown in the context of cryptography, whereas in [Li05b] one can find a thorough analysis of the dynamical degradation of a specific chaotic map and some ways to overcome this problem.

Problem 13. ***Lack of details in the description.*** *According to Kerckhoffs' principle, the security of a cryptosystem can not be based on the secrecy of its encryption and decryption procedures. Furthermore, the key of any cryptosystem has to be easy to establish and to exchange, and the key space must be defined in an explicit and clear way.*

The consecution of security through obscurity is something to avoid when design-

ing an encryption scheme. All the operations involved in the encryption/decryption procedures must be verbosely explained, and the secret key must be clearly specified along with an exact estimation of the size of the key space. The security of the cryptosystem must be only related to the difficulty of guessing the key, and it can not depend on the lack of knowledge about the inner operating of the encryption and decryption procedures. Moreover, this lack of details implies a lack of security because without a careful investigation of the whole cryptography community many security holes might not be able to be distinguished by the designers themselves. In Sec. 3.2 we have analyzed the loss of chaoticity in the cryptosystem defined in [Chee06]. Indeed, in that cryptosystem part of the key is given by a set of functions changing the values of the control parameters of a Hénon map as the plaintext is encrypted. The authors of [Chee06] do not define explicitly and rigorously those functions, which could result in a security flaw, as we have shown in [Arroyo08b] for the set of functions given by Eqs. (2.11)-(2.13). Another example of the kind of problem under consideration can be found in some encryption schemes built upon continuous-time chaotic systems. Certainly, when working with this type of chaotic systems it is necessary to use numerical methods to compute the chaotic orbits. The decryption procedure requires to generate the same chaotic orbits as in the encryption stage and, consequently, its computation must be done using the same numerical method and the same time step. Moreover, the influence of both the numerical method and the time step on the performance of the cryptosystem must be thoroughly evaluated. Let us take up again the cryptosystem defined in [Gao08a] (Case study 5.3.2). The masking stage of that cryptosystem is driven by a keystream derived from the orbits of Lorenz' and Chen's systems. In [Gao08a], the authors did not say anything about the time step τ of iterating the Lorenz and Chen systems. However, the randomness of the keystream is tightly dependent on the value of the time step. As an extreme example, if $\tau = 10^{-20}$, we will get a keystream of identical elements (according to the algorithm described in Sec. 2.3 of [Gao08a]).

5.5 Design rules

According to the above problems, we proceed with the concretion and systematization of the guidelines to observe when designing a chaos-based digital cryptosystem. These guidelines, that can be interpreted as the extension of the set of rules provided in [Alvarez06b], are the main conclusion of the work in [Alvarez07b; Arroyo08a; Arroyo09f; Arroyo08b; Arroyo09g; Arroyo08d; Arroyo09h; Arroyo08c; Arroyo09d; Rhouma09; Arroyo09e], i.e., the result of the practical application of the framework

described in Chapters 2-4 of this Thesis.

Rule 1. ***Exhaustive and rigorous definition of the chaotic encryption and decryption algorithms.***

The design of any encryption system must be guided by Kerckhoffs' principles, and thus the consecution of security through obscurity must be totally discarded. The designed cryptosystem must be easily reproducible, in order to make easy its implementation, use and further analysis. Indeed, assuring the security of an encryption procedure is a quite complex and non-closed problem, so the more people involved in the analysis, the more complete the security assessment is. Regarding specifically chaos-based cryptosystems, the encryption/decryption algorithms must assure control parameters determining the chaotic behavior of the selected maps. In addition, the final cryptosystems must be evaluated by means of the classical cryptanalytic framework (Sec. 1.2.2). It must be guaranteed that an attacker cannot get enough information about the underlying chaotic orbits, and thus she cannot carry out an estimation of control parameters and/or initial condition.

Rule 2. ***Avoid degradation of chaoticity by an exhaustive and rigorous definition of the key and the key space.***

In chaos-based cryptography is mandatory to specify clear and carefully the relationship between the secret key and the parameters determining the temporal evolution of the underlying chaotic maps, i.e., the control parameters and the initial conditions. In some cryptosystems either the control parameters or the initial conditions or both are part of the secret key, whereas in others they are just design parameters and, consequently, publicly known. Another possibility is that the secret key determines the values of the control parameters and initial conditions. In all situations it must assure that the underlying dynamical systems involved in the considered chaos-based cryptosystem evolves as required, i.e., in a chaotic way. In other words, the values of the control parameters used during encryption and decryption must determine positive values of the largest component of the LE. Furthermore, since the determination of LE entails some inaccuracies [Pastor97], it is highly advisable to analyze the chaoticity of orbits using auxiliary tools as the entropy measures referred in Sections 2.4, 2.5.1 and 2.5.2. Finally, either LE or the different entropy measures can bring to light a somehow one-to-one relationship between the rate of divergence of orbits and the control parameters. In this case, if a chaos-based cryptosystem allows an estimation of the rate of divergence, then it could be possible to estimate the control parameters, which represents a vulnerability of the cryptosytem being the control parameters part or determined by the secret key.

Rule 3. ***Selection of chaotic maps with high sensitivity to control parameter mismatch.***

The size of the key space of any cryptosystem must be large enough to avoid the feasibility of a brute-force attack. This is a common requirement of all encryption systems, and it has to be fulfilled in accordance with the computational capacity of any possible attacker. As it is pinpointed in [Alvarez06a, Rule 15], today's computer speed requires a key space of size larger than 2^{100}. As indicated by the previous rule, in digital chaos-based cryptography the specification of the key space is mainly guided by the calculation of the LE. Consequently, the resolution in the computation of the LE is a measure of the maximum number of possible keys, and thus an approximation of the size of the key space. To get a number of keys larger than $2^{100} \approx 10^{30}$, the resolution must be 10^{-30}. However, with that resolution, thousands of keys would become equivalent, unless there is a strong sensitivity to parameter mismatch. It implies that the concretion of the key space must be accompanied of an exhaustive analysis of the orbits generated for each value of the control parameters. Indeed, it must be tested that the orbits are different enough to assure that the encryption procedure possesses confusion and diffusion properties. Useful tools in this regarding are the statistical distance (see Sec. 2.6) and the MRE (see Sec. 2.5.2).

Rule 4. ***The selected chaotic map should not allow total characterization of its dynamics from a partial knowledge of this dynamics.***

The total characterization of the dynamics of a chaotic map requires the knowledge of the initial condition and the control parameters. When considering a chaos-based cryptosystem, it could be possible for an attacker to guess either the initial condition or some the control parameters. Upon the guessed information, the attacker could use some of the general attack strategies (Sec. 1.2.2) to get some additional information about the orbits of the underlying chaotic map. For some chaotic maps, this additional information and the guessed information drive to the estimation of the rest of parameters describing the dynamics of the map. For example, if the chaotic map selected for an encryption architecture is an unimodal map, and the encryption architecture allows to infer the symbolic sequences of the map through some attack, then the knowledge of the control parameter allows to recover the initial condition.

Rule 5. ***Analysis of the performance of chaotic orbits as source of entropy.***

From the point of view of cryptography, the appealing of chaos is mainly motivated by its random-like behavior. Actually, "the battle" of any cryptographer is to look for

sources of indetermination that can be further used to conceal the information. The design of a cryptosystem is the specification of a series of transformation procedures based on sources of indetermination and applied on the source of information. In chaos-based cryptography, all or some of the transformation procedures use chaos as source of indetermination. Since the security of the whole cryptosystem lies on the efficiency of each transformation procedure, the entropy must be evaluated. Again, the assessment must be done using the tools described in Sections 2.4, 2.5.1 and 2.5.2. Furthermore, this assessment can also be refined by considering every transformation procedure as a *Pseudo Random Number Generator*(PRNG). Upon this consideration, evaluation can be fulfilled using the battery of statistical tests of the National Institute of Standard & Technology (NIST) [NIST01]. Nevertheless, if chaos is used as base of a chaos-based stream cipher, then it is also necessary to analyze the possibility of reconstructing the symbolic dynamics in order to verify the feasibility of estimation for the control parameter(s) and initial conditions as it is done in Chapters 3 and 4.

Rule 6. ***Selection of chaotic maps guaranteing*** **avalanche effect.**

This rule is equivalent to the diffusion property, and it is intended to make the relationship between the key (or the plaintext) and the ciphertext as complex as possible. The goal is to erase any possible pattern or redundancy in the ciphertext, and thus to avoid inference of the secret key from the ciphertext. In the context of chaos-based cryptography, diffusion is connected to the local rate of divergence of orbits. As a result, chaotic maps with high values of LE must be selected. It is also possible to use chaotic maps with small LE if the encryption of each unit of plaintext is performed iterating several times the chaotic map. Nevertheless, it implies a reduction of the efficiency of the cryptosystem, and thus it is preferable to discretize the key space to guarantee the *avalanche effect*, i.e., the result of encrypting a plaintext with two slightly different keys must produce totally different ciphertexts. The tools for verification of the avalanche effect are the same used in the assessment of parameter mismatch, i.e., the statistical distance and the MRE. The discretization of the key space implies a reduction of its size, which could result in a degradation of the protection against brute-force attacks. A possible solution to this problem is to discretise the orbits of the chaotic maps instead of the key space. As we have shown in Sec. 3.2 for the skew tent map, this strategy determines an increasing of the LE and, consequently, of diffusion.

Rule 7. ***Chaotic maps with flat histograms and width of the phase space not depending on the control parameters must be used.***

If this requirement is satisfied, then the chaotic cryptosystem possesses the confusion property. If the underlying dynamical system evolves, as expected, chaotically, then it possesses the ergodic property and thus orbits are statistically independent of the control parameters and initial conditions. As a result, the ciphertext should be statistically undistinguishable from the output of a truly random function, and should be statistically the same for all the keys.

Rule 8. ***The ciphertext space must be defined in such a way that the reconstruction of the dynamics of the underlying chaotic maps is not possible.***

Ciphertexts of chaos-based cryptosystems must not leak information about the symbolic dynamics, the return map or any other shortcut to reconstruct the dynamics of the underlying chaotic maps.

Rule 9. ***The secret key of a chaos-based cryptosystem must not include the number of iterations of the underlying chaotic maps.***

If it is necessary to perform encryption through several rounds and several iterations of the underlying chaotic maps, then the number of encryption rounds and the number of iterations must be publicly known. They can not be considered as part of the secret key, since a mere analysis of the encryption/decryption time allows an estimation of those values.

Rule 10. ***Resistance to classical attacks.***

The cryptanalysis of chaos-based cryptosystems combined techniques from the theory of dynamical systems and from the cryptanalysis of conventional cryptography. In this concern, it must be verified the robustness of the cryptosystem against known-plaintext, chosen-plaintext, known-ciphertext, and chosen-ciphertext attacks. Specialized attacks must also be evaluated [Stamp07]. For digital chaos-based block ciphers resistance to differential [Szczepanski05] and linear cryptanalysis [Jakimoski01b] must be proved.

Rule 11. ***Resistance to application-specific attacks.***

The encryption of information with special features must be defined carefully in order to avoid the leaking of such features in the ciphertext. This is the case of digital images and videos. In digital images (videos) there exists an strong correlation between different pixels (transform coefficients), which can used to develop some effective correlation-based attacks.

5.6 Evaluation of some chaos-based encryption proposals

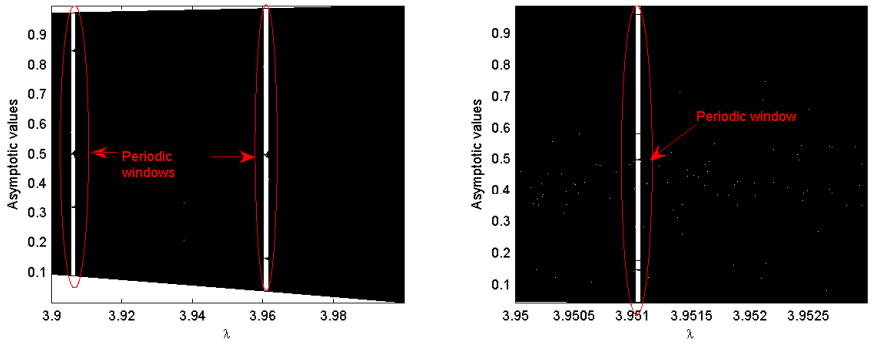
In this Thesis the process conducting to the above design rules is of *negative* nature. Indeed, we have analyzed a significative set of recent proposals in the field of chaos-based cryptography, we have established their main problems, and finally we have proposed a group of strategies to elude those problems. In other words, we have established what is insecure and, accordingly, we have recommended strategies to avoid it. As a consequence of the procedure carried out, one can think that chaos-based cryptography is intrinsically insecure. Indeed, all case studies proposed in this Thesis show security problems, but no "secure" chaos-based cryptosystem has been introduced. Therefore, the next step is to show some chaos-based cryptosystems that can be considered "secure". Before proceeding with the description of those "good" cryptosystems, it is necessary to establish what we mean by "secure" cryptosystem. In the context described along this Thesis, a secure cryptosystem is one that does not have any of the security flaws that we have pinpointed, i.e., one that satisfies a set of relevant rules among the group of rules given in the previous section; the subset of relevant rules is determined by the type of encryption architecture. Once the setting has been clarified, let us examine the level of "security" of the next three groups of chaos-based cryptosystems:

- Searching-based chaotic ciphers. This kind of chaotic cryptosystems has been explained and analyzed in Case study 3.5.1. Recalling, this type of cryptosystems split the phase space into a set of disjoint intervals. The number of disjoint intervals is given by the size of the alphabet of plaintexts, and each character of the alphabet is assigned to one interval of the phase space. Encryption is performed by iterating the underlying chaotic map and recording the number of iterations to land into the interval associated to each unit of plaintext. The most important part in the design of this class of cryptosystems is to find a chaotic map with a uniform probability distribution function. As a matter of fact, the main problem of the searching-based cryptosystems proposed in [Baptista98; Wang08c] is that they have been designed without considering Rule 7. In both cryptosystems the logistic map is conducting encryption, which erodes security. Therefore, logistic map must be replaced by other chaotic map with uniform probability distribution function. A possible candidate is the skew tent map (see Sec. 2.3). However, the selection of the skew tent map does not prevent from a chosen-ciphertext attack as the one described in Case study 3.5.1. Certainly, a chosen-ciphertext attack allows to get the symbolic

sequences of the skew tent map, which further enables to obtain an estimation of the control parameter from either the ratio between 0-bits and 1-bits, or the PDF of the order pattern #0 (Sec. 4.4). As a result, the skew tent map must also be discarded. The skew tent map is a *piecewise linear map*. Piecewise linear maps are defined by splitting the phase space into a set of M disjoint intervals. In each of those intervals the map is defined by a linear function. PieceWise Linear Chaotic Maps (PWLCM) possess a uniform probability distribution function, and a LE increasing as M does [Li03, Chapter 3]. Another important aspect of PWLCMs is that their computational complexity is low, which is very convenient for chaos-based cryptography. As a result, searching-based chaotic ciphers should be implemented using a PWLCM with $M > 2$. Nevertheless, the ciphertext of searching-based cryptosystems still leaks information about the dynamics of the PWLCMs. More specifically, even if the original logistic map is replaced by a PWLCM, its return map can be reconstructed using a chosen-ciphertext attack as it is done in [Skrobek08]. As a matter of fact, [Baptista98] violates Rule 8, and some additional improvement must be incorporated. A possible solution can be achieved by using the encryption architecture defined in [Huang05], but replacing the logistic map by a PWLCM. In this last encryption architecture, the plaintext is encrypted bit by bit, and each interval is assigned randomly to a 0-bit or a 1-bit instead of a character of the alphabet of plaintexts. Consequently, the number of iterations to encrypt a unit of plaintext is drastically reduced, and the dynamics of the underlying chaotic map cannot be reconstructed through a chosen-plaintext attack. Therefore, the cryptosystem [Huang05] with a PWLCM overcomes the problems of the previous searching based chaotic cipher, and simultaneously improves the efficiency of the encryption procedure.

- Chaos-based cryptosystems for image encryption. Image encryption is somehow different from text encryption due to some inherent features of images, such as bulk data capacity and high correlation among pixels. Therefore, digital chaotic ciphers like those in [Baptista98; Alvarez99] and traditional cryptographic techniques such as DES, IDEA and RSA [Menezes97; Stinson95] are no longer suitable for practical image encryption, especially for real-time communication scenarios. So far, many chaos-based image cryptosystems have been proposed [Chen04; Guan05; Pareek06b; Kwok07; Rhouma07; Wong08; Wang08d]. The major core of these encryption systems consists of one or several chaotic maps serving the purpose of either just encrypting the image or shuffling the

image and subsequently encrypting the resulting shuffled image. In [Wang08d] different chaotic maps are employed for image encryption. The plain-image is first permuted and later transformed through a keystream generated from the iteration of the logistic map. With respect to the second stage, the control parameter of the logistic map is part of the secret key. In [Wang08d] there is not a thoroughly definition of key space involving the control parameter of the logistic map. Indeed, the authors of [Wang08d] allow to use any value of the control parameter inside the interval $[3.9, 4]$, but it is well known that the bifurcation diagram of the logistic map has a dense set of periodic windows in that interval [Arroyo08a](see Fig. 5.6).



(a) (b)

Figure 5.6: Bifurcation diagram of the logistic map showing periodic windows: (a) $\lambda \in [3.9, 4]$; (b) $\lambda \in [3.95, 3.9523]$

Therefore, the cryptosystem proposed in [Wang08d] does not satisfy Rule 2. Nevertheless, the encryption architecture defined in [Wang08d] is a good reference to design new image encryption schemes based on chaos. Indeed, it is based on the concatenation of permutation and substitutions, which is the paradigm of conventional block ciphers [Menezes97]. A careful examination of the scheme given in [Wang08d] allows to conclude that it is secure against differential attacks. Furthermore, in [Wang08d] encryption is performed through several rounds. In each round the keystream is modified according to the plaintext, which represents an improvement of previous proposals of the authors [Chen04; Mao04]. As a result, Rule 10 is fulfilled by the cryptosystem defined in [Wang08d], being the selection of the logistic map the main problem of this cryptosystem.

- Block ciphers with dynamical S-Boxes from chaos. In this scenario chaotic maps are used to define the S-Boxes of conventional block ciphers [Menezes97]. S-

boxes are the elements implementing the non-linear transformation of the plaintext, and they are created either randomly or algorithmically. In [Kocarev01b; Jakimoski01b; Masuda06] the S-Boxes are generated by iterating and discretizing chaotic maps. The rules concerning this kind of cryptosystems are Rule 10 and Rule 2. Indeed, it has been verified that the resulting cryptosystems are vulnerable against the typical attacks on conventional block ciphers. In this sense, the authors of [Kocarev01b; Jakimoski01b] verify that the S-boxes obtained through the iteration and discretization of the selected chaotic maps resist the *differential and linear cryptanalysis*. Furthermore, the dynamical systems involved in the generation of the S-boxes are always working in chaotic regime (Rule 2), which finally confirms that the designed cryptosystems can be considered secure.

5.7 Concluding remarks

In this Chapter we have explained the main security problems in digital chaos-based cryptography. We have focused the attention on the problems derived from an inappropriate selection of the underlying chaotic maps, but we have also discussed some problems derived from the encryption architectures and the cryptosystem's implementation. A group of designing rules has been proposed as a methodology to avoid the previous underlined problems. Finally, the suitability of the design rules has been exemplified through the evaluation of different recent chaos-based cryptosystems. As a result of that analysis, we can conclude that the security of a chaos-based cryptosystem is preserved by using the encryption architectures of conventional cryptography, being chaos the origin of the non-linearities demanded by those encryption architectures. This is the main lesson learned from the analysis of chaotic cryptosystems. There is no need to invent a new paradigm, since conventional cryptography embodies all the methodologies and rules to design a good cryptosystem. Therefore, the first step when designing a chaos-based cryptosystem is to fully understand the concepts and standards used by cryptographers. As a matter of fact, only from a complete comprehension of the cryptographic corpus it is feasible to extract from chaos all its potential as support of encryption procedures. Nevertheless, to extract that potentiality it is necessary to know thoroughly the dynamics of chaos. Summing up, the cryptographic corpus highlights what cryptography expects from chaos, whereas the theory of chaotic systems reveals how chaos can be articulated to satisfy the cryptographic expectations.

Chapter 6

Conclusions and future work

6.1 Conclusions of this Thesis

The invention of writing was the dawn of the information revolution. This great technological advance allowed to overcome the barriers of time and distance when sharing ideas and news. Nevertheless, it entailed a serious problem when the intention was to share information with an specific reader or receiver. To assure selective reading, different strategies were invented to transform the written information into a gibberish. This transformation was dependent on an external parameter named (secret) key, which was known only by the ones writing the information and those allowed to read it. This was the beginning of *cryptography*. Simultaneously, different strategies were conceived to elude the security of the transformation procedures and, consequently, recover the original information without knowing the secret key. Originally information was hidden by either simple permutations or substitutions of written characters. Nevertheless, those operations were very easy to overcome for an illegitimate reader, and more complex encryption methodologies had to be designed. Upon the scene depicted by the set of the different encryption proposals, in 1949 Shannon defined the basics of *the theory of perfect secrecy*. According to Shannon, the perfect concealing of information requires the interleaving of good procedures of *confusion* and *diffusion* of information. Modern *symmetric ciphers* (or *secret key ciphers*) are based on those principles. Conventionally, number theory and abstract algebra are the foundation of the methodologies implementing confusion and diffusion of information. However, since 1990's many researchers have worked on developing confusion and diffusion by means of chaotic systems. Apparently the characteristics of chaotic dynamics can be connected to the requirements of cryptography and, consequently, chaotic cryptosystems can be designed following the standards of conventional cryptography.

Along this Thesis the goal has been to emphasize the possibility of accomplishing

the needs of cryptography through the virtues of chaos. If the foundations of conventional cryptography arises from number theory, chaos-based cryptography is based on the possibility of conforming non-linear transformations of the *plaintext* using chaotic orbits. From this point of view, the security of chaos-based encryption procedures is very related to the possibility of reconstructing those orbits from known information. In this sense, our strategy has been to clarify the contexts where it is possible to get the control parameters and initial condition that originate a certain chaotic orbit. When attacking a cryptosystem, we explore if it is possible to circumvent the concealing of information according to four different scenarios:

- Only the output of the cryptosystem is known.
- Some outputs and inputs of the cryptosystem are known.
- We can select some inputs of the cryptosystem and calculate the corresponding outputs.
- We can choose some output of the cryptosystem and determine the corresponding inputs.

Regarding chaos-based cryptography, the vulnerability of a cryptosystem is proven if it is possible to connect some or several of the above scenarios with the contexts allowing the estimation from chaotic orbits of initial condition and/or control parameters. Strictly speaking, it is not enough to show the impossibility of such linking to conclude the cryptographic quality of a chaos-based encryption proposal. As a matter of fact, it is also required to examine thoroughly the inner aspects of the encryption architecture. In this sense, the encryption architecture might include elements from chaos theory, but also from other fields as number theory. In this Thesis we have assumed that those other fields are analyzed by means of the general methodologies of conventional cryptography and, consequently, we have focused the work on the specificity of the design of chaotic cryptosystems, i.e., the evaluation of chaotic orbits as bearers of strategies to *diffuse* and *confuse* information.

The potentiality of chaotic orbits as procedures of diffusion of information is given by the local divergence of chaos. As we have settled in Chapter 2, the local divergence of chaotic systems is measured by means of the Lyapunov exponent or LE. Chaotic maps involved in chaos-based cryptosystems must have positive maximum LE, and we have shown the consequences of a neglect of this respect through the analysis of the cryptosystem described in [Chee06] (Case study 2.2.1 and the corresponding cryptanalytical work in [Arroyo08b]). On the other hand, the achievement of confusion

through chaotic orbits is not so "easy" to clarify as diffusion. Certainly, confusion is related to the level of uncertainty associated to chaotic orbits, but also is very dependent on the feasibility of modeling such uncertainty by means of chaotic dynamics. The level of uncertainty of a source of information is computed by measures of entropy. In this Thesis we have proposed different measures of entropy, in order to better clarify how chaotic orbits can be manipulated to conceal information. This being the case, entropy has been calculated through *generating partitions* (*Shannon's, Tsallis'*, and *n-gram conditional entropy*), but also by means of a characterization of chaos in the time-frequency domain (*Wavelet Entropy* and *MultiResolution Entropy*). Of course, the higher measure of entropy, the better performance from the perspective of confusion property. Nevertheless, some measures of entropy highlight a one-to-one or few-to-one relation with respect to the control parameters, which could represent a security problem for some chaos-based cryptosystems. Therefore, it is highly advisable to use measures of entropy as guide during the design of a chaos-based cryptosystem, since they can be very helpful when deciding how to build up ciphertexts from chaotic orbits. Moreover, it is very interesting the information obtained from the assessment of the statistical complexity of chaotic orbits. The skeleton of chaos is a dense set of *unstable periodic orbits* or *UPOs*, and some chaotic maps are associated to an entropy that increases as the number of UPOs does. Therefore, it is very convenient to handle this kind of relationship and, consequently, we have proposed to quantify the *statistical complexity* of chaotic orbits, through *Jensen's divergence*, and the *statistical distance* between orbits by means of *Wootters' distance*; in this sense, it is very meaningful the study we have performed about the potentiality of unimodal maps as base of stream ciphers, according to the encryption scheme described in [Kurian08] (Case study 2.6.1 with corresponding cryptanalytical work in [Arroyo09c]). In this analysis we show that the statistical distance between keystreams generated from very different values of the control parameter is large, whereas the one between keystreams generated from close values of the control parameter is small. Moreover, the statistical distance decreases as the difference between the control parameters does. Consequently, Wootters' distance can be used to get an estimation of the control parameter of the chaotic maps involved in the cryptosystem defined in [Kurian08].

Entropy is not the only indicator to confirm confusion property. Confusion also demands chaotic orbits with an "neutral" statistical behavior with respect to control parameters and initial condition. Indeed, if the histograms of chaotic orbits leak information about the control parameters, then in some contexts it could be possible for an attacker to infer them. An example of such type of contexts is depicted when

cryptanalyzing [Pisarchik06] (Case study 2.3.1 and the corresponding cryptanalytical work in [Arroyo08d]). The study of this cryptosystem has allowed us to highlight the importance of defining rigorously the ciphertexts of chaos-based cryptosytems. In this regard, also our cryptanalytical works [Arroyo09g; Arroyo09f] on the cryptosystems proposed in [Ling07; Wang08c] have been very useful (Case study 5.3.1 and Case study 3.5.1). Accordingly, security problems could arise if the *ciphertext* is conformed from chaotic orbits straightforwardly, but also if it is given by *coarse-grained* versions of the orbits. In this sense, we have studied the *symbolic dynamics* and *order patterns* of unimodal maps (Chapters 3-4). It is well known the relationship between the *symbolic sequences* of unimodal maps and the associated control parameter. In [Arroyo09a] we point out that the probability distribution of the order patterns of unimodal maps is also related to the control parameter. Accordingly, we have shown how both symbolic dynamics and order patterns can be used to estimate the control parameter and/or the initial condition from the symbolic sequences of unimodal maps, which confirms them as very helpful for the design and analysis of chaos-based cryptosystems. Since unimodal maps have been broadly used in the context of chaos-based cryptography, the proposed estimation methods reveal a very serious security problem. Furthermore, the methodology employed in the concretion of the estimation methods can be very useful as a paradigm to either analyze other chaotic maps, and conclude the adequacy of a chaotic map to encryption architectures whose security depends on its symbolic dynamics.

The work described in this Thesis is not a mere list of mathematical tools, it also embodies a series of case studies, being the result of our activity in the cryptanalysis of chaos-based cryptosystems [Arroyo08b; Arroyo09g; Arroyo09h; Arroyo09f; Arroyo09f; Arroyo09c]. These studies have been used to illustrate some of the mathematical tools proposed in this Thesis, but also to detect the main problems in chaos-based cryptosystems. Those problems are basically derived from a selection of chaotic maps not taking into account their dynamical properties. The key space and the performance of any chaos-based cryptosystem are very dependent on the "quality" of the chaotic maps selected as "heart" of the encryption procedure. In order to guarantee a correct selection of chaotic maps, we have made explicit a set of design rules in Chapter 5. In this regard, the main goal has been to point out that chaos-based cryptography is not a methodology apart from conventional cryptography, but a branch in cryptography that, roughly speaking, uses chaos instead of number theory as source of entropy. The paradigm that any designer of chaos-based cryptosystems must respect is given by the recommendations of conventional cryptography, plus the set of mathematical tools and critical contexts defined along this Thesis.

As it has been pinpointed at the beginning of this Section, chaos is introduced in cryptography to define new strategies of confusion and diffusion of information. The main contribution of this Thesis has been the concretion of a set of procedures to test if chaotic dynamics do really lead to those confusion and diffusion properties. Furthermore, those procedures are of practical nature, since they allow to confirm what cryptography expects and demands from cryptography in a practical environment, i.e, when working with finite precision arithmetics. Indeed, in a finite precision context the dynamical properties of chaos are eroded, which could further implies a degradation of the accomplishment of the needs of cryptography. This being the case, the battery of mathematical indicators defined along this Thesis must be used to assess the distance between the "factual" chaotic behavior and the requirements of cryptography. In a practical environment chaos cannot be assumed without previous evaluation, but also it cannot be assumed that chaos embodies confusion and diffusion properties without prior examination.

6.2 Contributions of this Thesis

In this Thesis we have described a series of mathematical tools to establish the link between the characteristics of chaotic systems and the confusion and diffusion properties of encryption schemes. The association between diffusion and the Lyapunov exponent is well known in the context of chaos-based cryptography, but the procedures to assess confusion are not so well known. To fulfill this need, we have introduced the following set of mathematical tools:

1. Measures of entropy. The potentiality of chaotic orbits as mechanisms bearing the encryption of information depends on the level of entropy of such orbits. This level of entropy depends on the dynamics of chaotic systems, but also on how encryption architectures transform chaotic orbits to conceal information. Therefore, we must use as many measures of entropy as possible. In this Thesis we have proposed to measure entropy using not only Shannon's measure, but also non-extensive measures as the one proposed by Tsallis. We have also shown how useful the n-gram conditional entropy is to decide the size of the units of plaintext. Certainly, the n-gram conditional entropy decreases as n (here assumed as the size of the units of plaintext) increases, which could seem negative for encryption. Nevertheless, small values of n could lead to a n-gram conditional entropy being a bijective function with respect to a control parameter, as we have shown for the case of the logistic map and the skew tent map. Moreover, for a given value of n, it is possible to discern the intervals of the control

parameters space where the n-gram conditional entropy is a bijective function of a control parameter. Since our goal is to elude any critical context allowing the estimation of control parameters, those regions of the control parameters space should be avoided. As a result, the n-gram conditional entropy is also a useful indicator when defining the key space of chaos-based cryptosystems.

2. Time-frequency analysis of chaotic orbits. We have shown that the Wavelet Transform is another important tool when designing and analyzing digital chaos-based cryptosystems. Certainly, the Wavelet Transform allows to define different measures of entropy, as the Wavelet Entropy and the MultiResolution Entropy, without knowing the generating partition of chaotic maps. Moreover, we have pinpointed that the MultiResolution Entropy enables the detection of changes in the control parameters, which reveals a critical context for those encryption architectures where the control parameters of the underlying chaotic maps change as encryption is performed.

3. Statistical complexity. For some chaotic maps the entropy of the associated orbits is very related to the density of the underlying Unstable Periodic Orbits or UPOs. As a consequence, an increase of the entropy informs about an increase of the number of UPOs. The tool to measure this relationship is the statistical complexity. In this Thesis we have used the statistical complexity defined using Jensen's measure of divergence and some measure of entropy. We have shown that the statistical complexity of the logistic map is a one-to-one function with respect to the control parameter, when the control parameter is selected to have chaotic behavior. Therefore, the statistical complexity is another very important tool when examining the adequacy of a chaotic map for a given encryption architecture. If the statistical complexity of the chaotic map can be measured manipulating somehow the encryption architecture, then the statistical complexity should not be a bijective function of a control parameter (supposing that the chaotic map has more than one control parameter).

4. Statistical distances. As we have shown in this Thesis, the analysis of the histograms of chaotic orbits is very useful when assessing the cryptographic quality of a chaotic map. If the shape of the histograms changes as some control parameter does, then a given value of the control parameter could be estimated through the statistical distance between the histogram associated to the given value of the control parameter, and the histograms generated from a set of candidates values for the control parameter. In this Thesis we have used

the statistical distance defined by Wootters, and we have shown its virtues as a tool for the cryptanalysis of keystreams derived from the iteration of chaotic maps.

5. Application of Gray codes to the estimation of the control parameter and initial condition of unimodal maps. In this Thesis we have shown that the Theory of Symbolic Dynamics reveals a critical context to handle when designing chaos-based cryptosystems. In this regard, we have shown that symbolic sequences of unimodal maps can be interpreted as Gray codes. Furthermore, any Gray code can be transformed into a number called Gray Ordering Number or GON. The GON defines a few-to-one relationship with respect to the control parameter. We have shown how to use that relationship to estimate the control parameter from a given symbolic sequence, when working with unimodal maps. Moreover, if the control parameter of a unimodal map is known, the initial condition associated to a Gray code can be inferred without error. Although our analysis has been focused on unimodal maps, it depicts a critical context when considering encryption architectures leaking the symbolic sequences of the underlying chaotic maps. For those encryption architectures it must be guaranteed that it is not possible to build up a one-to-one (or a few-to-one) relationship between the symbolic sequences of the selected chaotic map and any of the associated control parameters.

6. Application of order patterns to the estimation of the control parameter of unimodal maps. The knowledge of the critical point of unimodal maps is a requirement to perform the estimation method based on the GON. Nevertheless, we have shown that it is possible to perform such estimation using the probability distribution function of the order patterns of unimodal maps. As a matter of fact, if the relative frequency of an order pattern in a chaotic orbit provides a one-to-one or a few-to-one relationship with respect to the control parameter, then the control parameter can be estimated. Hence, the study of order patterns of a chaotic map depicts another critical context to consider when designing a digital chaos-based cryptosystem.

The concretion of the mathematical framework described in this Thesis is the result of a thorough analysis of a meaningful set of digital chaos-based cryptosystems. This analysis has been specially performed for the following digital chaos-based cryptosystems:

7. In 2006, Chee et al. proposed a chaotic cryptosystem based on the Hénon

map. In this Thesis we have emphasized the lack of a description about the key space of this cryptosystem, and we have also indicated the difficulty of finding new keys when working with the Hénon map. Finally we have shown that it is possible to break the cryptosystem when the keys are not selected properly using a known-plaintext attack and assuming a partial knowledge of the key.

8. The security of the image encryption scheme proposed by Gao et al. in 2008 has been analyzed in detail. It has been shown that the equivalent secret key can be recovered in a chosen-plaintext attack with only $\lceil \log_{256}(MN) \rceil + 1$ chosen plain-images, being M and N the width and the height of the plain-images respectively. In addition, some other defects have also been distinguished in the scheme under study. Among those defects, it is necessary to emphasize the one concerning the encryption speed, since it informs about the non-convenience of continuous-time chaotic systems for implementing fast encryption procedures.

9. In this Thesis we have analyzed the security properties of the cryptosystem proposed by Ling et al. in 2007. We have shown that there exists a great number of weak keys derived from the fact that the logistic map is not always chaotic. In addition, the cryptosystem is very weak against a known-plaintext attack in the sense that the secret key can be totally recovered using a very short plaintext.

10. In 2006, Pisarchik et al. proposed encryption scheme based on the logistic map. We have emphasized some problems concerning the key space definition and the implementation of the cryptosystem using floating-point operations. We have also shown how it is possible to reduce considerably the key space through a ciphertext-only attack. Moreover, a timing attack allows the estimation of part of the key due to the existent relationship between this part of the key and the encryption/decryption time.

11. In 2008, Wang et al. defined a cryptosystem based on the ergodicity property of the logistic map. A chosen-ciphertext attack has been described, which can recover the secret key of the cryptosystem by exploiting the theory of symbolic dynamics.

12. In 2008, Kurian et al. defined a stream cipher whose keystream is basically a symbolic sequence of the (one-parameter) logistic map or of the skew tent map. We have shown that the Wootters' statistical distance can be used to discern between the keystreams of the logistic map and those corresponding to the skew

tent map. Once the underlying chaotic map is identified, the control parameter and the initial condition can be estimated using the Theory of Symbolic Dynamics and the analysis of the probability distribution functions of order patterns. From a a general point of view, the results of this cryptanalysis hint to the fact that symbolic sequences of unimodal maps are insecure when used as keystreams.

As a result of our cryptanalytical work and the mathematical framework we have defined along this Thesis, it is possible to conclude a set of recommendations to design a "good" digital chaos-based cryptosystem:

13. Definition of a set of rules for the design of digital chaos-based cryptosystems. When designing a digital chaos-based cryptosystem it must be guaranteed that it is not possible to apply successfully any of the cryptanalysis tools and procedures explained along this Thesis. Furthermore, the security of the final cryptosystem cannot be guaranteed unless it is also examined using the tools and procedures of conventional cryptography. Indeed, we must not forget that chaos-based cryptography is a branch of cryptography that uses chaotic systems as sources of entropy and, consequently, it must respect the same standards and requirements that conventional cryptography does.

6.3 Future work

The main points to investigate, as an extension of the research work covered by this Thesis, are:

- **Theory of discrete chaos**. The final concretion of the framework defined in this paper requires a further investigation of the theory of discrete chaos. In this regard the work will be focused on improving and enlarging the tools described in this Thesis according to the theory introduced in [Kocarev06; Amigó07; Amigó07b; Amigo07a; Amigó08a].

- **Application of the theory of symbolic dynamics and order patterns of unimodal maps to other maps.** In this Thesis symbolic dynamics and order patterns have been applied to the study of a class of unimodal maps. A broader scope can and must be depicted using the work in [Hansen92; Daw03; Keller03; Keller05; Keller07; Bandt05; Pethel06; Bandt07; Wang08b] and the theory explained in [Hao98; Lind95; Kitchens97].

- **Study of the applicability of chaotic dynamics to public-key cryptography** In this Thesis only symmetric encryption schemes have been considered. Nevertheless, it is also possible to design public key encryption strategies using chaotic systems [Kocarev03; Bergamo05; Kocarev05; Schmitz08]. Some of the proposals in the field of chaos-based public key cryptography are based on the Mandelbrot set [Alia07; Alia08], and thus future work will be focused on studing those proposals by means of our work about the inner structure of unimodal maps [Pastor06; Pastor07a; Alvarez07a; Pastor07b; Pastor07c; Pastor07d; Alvarez07b; Pastor08; Romera08; Arroyo09a].

- **Study of other sources of chaos and their application to cryptography.** Recently optical systems have been used as sources of entropy to encrypt information [Argyris05], although not many proposals are secure [Udaltsov03]. Future work will be focused on the analysis of the scheme proposed in [Fernandez08b; Fernandez08a] in order to verify its application to generate chaotic signals for encryption of information. Another topic to further investigate is arithmetic coding. In [Nagaraj08; Nagaraj09; Li09] it is shown that arithmetic coding can be studied by means of the theory of dynamical systems. Moreover, it is shown how to use arithmetic coding to generate robust chaos, which further contributes to generate PRNG with very long periods.

- **Cryptanalysis of known digital chaotic ciphers.** Cryptanalysis is fundamental for the progress and improvement of cryptography. Since our work is focused on promoting a better understanding of the interaction between chaos and cryptography, we must apply to the analysis of new cryptosystems the theoretical conclusions resulting from the different areas of research in chaos. Indeed, every single progress in the theory of discrete chaos, symbolic dynamics, order patterns or the analysis of chaotic time-series is not useful for cryptography if it can not be applied to the analysis of chaos-based cryptosystems.

- **Analysis of conventional encryption schemes by means of the theory of dynamical systems**. Another important topic to examine is the possibility of applying the tools that we have described in this Thesis to conventional encryption schemes. Certainly, the theory of dynamical systems can be helpful when analyzing the properties of conventional block [Kocarev04; Ruggiero04] and stream ciphers [Millérioux08]. Tools like the Lyapunov exponent, or the different measures of entropy proposed in this Thesis could be useful to study conventional cryptosystems. In other words, in this Thesis we have worked on

discerning how close the virtues of chaos are to the needs of cryptography, and future work will be on establishing the relation between the permutations and non-linearities of conventional ciphers, and chaotic behavior.

Bibliography

[Al-Assaf04] Y. Al-Assaf and W. M. Ahmad (2004). Parameter identification of chaotic systems using wavelets and neural networks. *International Journal of Bifurcation and Chaos in Applied Sciences and Engineering*, 14(4):1467–1476.

[Alia07] M. A. Alia and A. B. Samsudin (2007). A new digital signature scheme based on Mandelbrot and Julia fractal sets. *American Journal of Applied Sciences*, 4(11):850–858.

[Alia08] M. A. Alia and A. B. Samsudin (2008). Fractal Mandelbrot and Julia zero-knowledge proof of identity. *Journal of Computer Science*, 4(5):408–414.

[Alvarez98] Gonzalo Alvarez, Miguel Romera, Gerardo Pastor, and Fausto Montoya (1998). Gray codes and 1D quadratic maps. *Electronic Letters*, 34(13):1304–1306.

[Alvarez99] E. Alvarez, A. Fernández, P. García, J. Jiménez, and A. Marcano (1999). New approach to chaotic encryption. *Phys. Lett. A*, 263(4-6):373–375.

[Alvarez03a] Gonzalo Alvarez, F. Montoya, and G. Pastor (2003). Cryptanalysis of a discrete chaotic cryptosystem using external key. *Physics Letters A*, 319:334–339.

[Alvarez03b] Gonzalo Alvarez, Fausto Montoya, Miguel Romera, and Gerardo Pastor (2003). Cryptanalysis of an ergodic chaotic cipher. *Physics Letters A*, 311:172–179.

[Alvarez04a] Gonzalo Alvarez and S. Li (2004). Breaking network security based on synchronized chaos. *Computer Communications*, 27(16):1679–1681.

[Alvarez04b] Gonzalo Alvarez, F. Montoya, M. Romera, and G. Pastor (2004). Breaking a secure communication scheme based on the phase synchronization of chaotic systems. *Chaos*, 14(2):274–278.

[Alvarez04c] Gonzalo Alvarez, F. Montoya, M. Romera, and G. Pastor (2004). Breaking parameter modulated chaotic secure communication system. *Chaos, Solitons & Fractals*, 21(4):793–797.

[Alvarez04d] Gonzalo Alvarez, F. Montoya, M. Romera, and G. Pastor (2004). Breaking two secure communication systems based on chaotic masking. *IEEE Transactions on Circuits & Systems II*, 51(10):505–506.

[Alvarez04e] Gonzalo Alvarez, F. Montoya, M. Romera, and G. Pastor (2004). Cryptanalyzing a discrete-time chaos synchronization secure communication system. *Chaos, Solitons & Fractals*, 21(3):689–694.

[Alvarez04f] Gonzalo Alvarez, F. Montoya, M. Romera, and G. Pastor (2004). Keystream cryptanalysis of a chaotic cryptographic method. *Computer Physics Communications*, 156:205–207.

[Alvarez04g] Gonzalo Alvarez, Fausto Montoya, Miguel Romera, and Gerardo Pastor (2004). Cryptanalysis of dynamic look-up table based chaotic cryptosystems. *Physics Letters A*, 326:211–218.

[Alvarez05a] Gonzalo Alvarez, L. Hernández, J. Munoz, F. Montoya, and S. Li (2005). Security analysis of communication system based on the synchronization of different order chaotic systems. *Physics Letters A*, 345(4):245–250.

[Alvarez05b] Gonzalo Alvarez, Shujun Li, Fausto Montoya, Miguel Romera, and Gerardo Pastor (2005). Breaking projective chaos synchronization secure communication using filtering and generalized synchronization. *Chaos, Solitons & Fractals*, 24(3):775–783.

[Alvarez06a] G. Alvarez and S. Li (2006). Breaking an encryption scheme based on chaotic baker map. *Physics Letters A*, 352(1-2):78–82.

[Alvarez06b] Gonzalo Alvarez and Shujun Li (2006). Some basic cryptographic requirements for chaos-based cryptosystems. *Int. J. Bifurc. Chaos*, 16(8):2129–2151.

[Alvarez07a] Gonzalo Alvarez, David Arroyo, and Juana Nunez (2007). Aplicaciones de los códigos de gray a la criptografía caótica. In *NoLineal 2007, Escuela Universitaria de Magisterio de Ciudad Real*.

[Alvarez07b] Gonzalo Alvarez, David Arroyo, and Juana Nunez (2007). 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)*. IEEE IPACS, Potsdam, Germany. URL http://lib.physcon.ru/?item=1358.

[Amigó07] J.M. Amigó, L. Kocarev, and J. Szczepanski (2007). Theory and practice of chaotic cryptography. *Physics Letters A*, 366(3):211 – 216. ISSN 0375-9601.

[Amigó06] J. M. Amigó, L. Kocarev, and J. Szczepanski (2006). Order patterns and chaos. *Physics Letters, Section A: General, Atomic and Solid State Physics*, 355(1):27–31.

[Amigo07a] J.M. Amigo, L. Kocarev, and J. Szczepanski (2007). Discrete Lyapunov exponent and resistance to differential cryptanalysis. *Circuits and Systems II: Express Briefs, IEEE Transactions on*, 54(10):882–886. ISSN 1549-7747.

[Amigó07b] J.M. Amigó, L. Kocarev, and I. Tomovski (2007). Discrete entropy. *Physica D*, 228:77–85.

[Amigó07c] José María Amigó, Samuel Zambrano, and Miguel A. F. Sanjuán (2007). True and false forbidden patterns in deterministic and random dynamics. *Europhysics Letters*, 79:50001–p1, –p5.

[Amigó08a] José M. Amigó, Ljupco Kocarev, and Janusz Szczepanski (2008). On some properties of the discrete lyapunov exponent. *Physics Letters A*. In Press.

[Amigó08b] José María Amigó, Sergi Elizalde, and Matthew B. Kennel (2008). Forbidden patterns and shift systems. *Journal of Combinatorial Theory, Series A*, 115:485–504.

[Argyris05] Apostolos Argyris, Dimitris Syvridis, Laurent Larger, Valerio Annovazzi-Lodi, Pere Colet, Ingo Fischer, Jordi García-Ojalvo,

Claudio R. Mirasso, Luis Pesquera, and K. Alan Shore (2005). Chaos-based communications at high bit rates using commercial fibre-optic links. *Nature*, 438:343–346.

[Arroyo08a] David Arroyo, Gonzalo Alvarez, and Veronica Fernandez (2008). On the inadequacy of the logistic map for cryptographic applications. In L. Hernandez and A. Martin, editors, *X Reunión Española sobre Criptología y Seguridad de la Información (X RECSI)*, pages 77–82, (ISBN 978–84–691–5158–7). Universidad de Salamanca, Salamanca, Spain.

[Arroyo08b] David Arroyo, Gonzalo Alvarez, Shujun Li, Chengqing Li, and Juana Nunez (2008). Cryptanalysis of a discrete-time synchronous chaotic encryption system. *Physics Letter A*, 372(7):1034–1039.

[Arroyo08c] David Arroyo, Rhouma Rhouma, Gonzalo Alvarez, Veronica Fernandez, and Safya Belghith (2008). On the skew tent map as base of a new image chaos-based encryption scheme. In Álvar Ibeas and Jaime Gutiérrez, editors, *Second Workshop on Mathematical Cryptology*, pages 113–117. Universidad de Cantabria, Santander, Spain.

[Arroyo08d] David Arroyo, Rhouma Rhouma, Gonzalo Alvarez, Shujun Li, and Veronica Fernandez (2008). On the security of a new image encryption scheme based on chaotic map lattices. *Chaos: An Interdisciplinary Journal of Nonlinear Science*, 18:033112, 7 pages.

[Arroyo09a] David Arroyo, Gonzalo Alvarez, and José María Amigó (2009). Estimation of the control parameter from symbolic sequences: Unimodal maps with variable critical point. *Chaos: An Interdisciplinary Journal of Nonlinear Science*, 19:023125, 9 pages.

[Arroyo09b] David Arroyo, Gonzalo Alvarez, and José María Amigó (2009). Estimation of the control parameter of a map through the analysis of its order patterns. In *ICCSA 2009*. Le Havre, France.

[Arroyo09c] David Arroyo, Gonzalo Alvarez, José María Amigó, and Shujun Li (2009). Cryptanalysis of a family of self-synchronizing chaotic stream ciphers. URL http://arxiv.org/abs/0903.2928, submitted to Signal Processing on 17 March, 2009.

[Arroyo09d] David Arroyo, Gonzalo Alvarez, and Veronica Fernandez (2009). A basic framework for the cryptanalysis of digital chaos-based cryptography. In *Sixth International Multi-Conference on Systems, Signals and Devices*. Djerba, Tunisia.

[Arroyo09e] David Arroyo, Gonzalo Alvarez, and Shujun Li (2009). Some hints for the design of digital chaos-based cryptosystems: lessons learned from cryptanalysis. In *Second IFAC Conference on Analysis and Control of Chaotic Systems*. Queen Mary, University of London.

[Arroyo09f] David Arroyo, Gonzalo Alvarez, Shujun Li, Chengqing Li, and Veronica Fernandez (2009). Cryptanalysis of a new chaotic cryptosystem based on ergodicity. *International Journal of Modern Physics B*, 23(5):651–659.

[Arroyo09g] David Arroyo, Chengqing Li, Shujun Li, and Gonzalo Alvarez (2009). Cryptanalysis of a computer cryptography scheme based on a filter bank. *Chaos, Solitons and Fractals*, 41:410–413.

[Arroyo09h] David Arroyo, Chengqing Li, Shujun Li, Gonzalo Alvarez, and Wolfgang A. Halang (2009). Cryptanalysis of an image encryption scheme based on a new total shuffling algorithm. *Chaos, Solitons and Fractals*, 41(5):2613–2616.

[Bakker00] R. Bakker, J. C. Schouten, C. Lee Giles, F. Takens, and C. M. Van den Bleek (2000). Learning chaotic attractors by neural networks. *Neural Computation*, 12(10):2355–2383.

[Bandt02] Christoph Bandt and Bernd Pompe (2002). Permutation entropy: A natural complexity measure for time series. *Phys. Rev. Lett.*, 88(17):174102.

[Bandt05] C. Bandt (2005). Ordinal time series analysisis. *Ecological Modelling*, 182:229–238.

[Bandt07] Christoph Bandt and Faten Shiha (2007). Order patterns in time series. *Journal of Time Series Analysis*, 28(5):646–665.

[Banerjee98] Soumitro Banerjee, James A. Yorke, and Celso Grebogi (1998). Robust chaos. *Physical Review Letters*, 80:14.

[Baptista98] M. S. Baptista (1998). Cryptography with chaos. *Physics Letters A*, 240(1-2):50–54.

[Bergamo05] P. Bergamo, P. D'Arco, A. De Santis, and L. Kocarev (2005). Security of public-key cryptosystems based on chebyshev polynomials. *IEEE Transactions on Circuits and Systems I: Regular Papers*, 52(7):1382–1393.

[Beyer86] W.A. Beyer, R.D. Mauldin, and P.R. Stein (1986). Shift-maximal sequences in function iteration: Existence, uniqueness and multiplicity. *J. Math. Anal. Appl.*, 115:305–362.

[Billings01] L. Billings and E. M. Bollt (2001). Probability density functions of some skew tent maps. *Chaos, solitons and fractals*, 12(2):365–376.

[Billings05] S.A. Billings and Hua-Liang Wei (2005). A new class of wavelet networks for nonlinear system identification. *Neural Networks, IEEE Transactions on*, 16(4):862–874. ISSN 1045-9227.

[Brin03] Michael Brin and Garret Stuck (2003). *Introduction to dynamical systems*. Cambridge University Press.

[Brumley03] David Brumley and Dan Boneh (2003). Remote timing attacks are practical. In *SSYM'03: Proceedings of the 12th conference on USENIX Security Symposium*, pages 1–14. USENIX Association, Berkeley, CA, USA.

[Buhl05] Michael Buhl and Matthew B. Kennel (2005). Statistically relaxing to generating partitions for observed time-series data. *Physical Review E*, 71:046213:1–14.

[Buhl07] Michael Buhl and Matthew B. Kennel (2007). Globally enumerating unstable periodic orbits for observed data using symbolic dynamics. *Chaos: An Interdisciplinary Journal of Nonlinear Science*, 17(3):033102.

[Cao95] Liangyue Cao, Yiguang Hong, Haiping Fang, and Guowei He (1995). Predicting chaotic time series with wavelet networks. *Physica D: Nonlinear Phenomena*, 85(1-2):225 – 238.

[Chee06] Chin Yi Chee and Daolin Xu (2006). Chaotic encryption using dicrete-time synchronous chaos. *Physics Letters A*, 348(3-6):284–292.

[Chen99] Guanrong Chen and Tetsushi Ueta (1999). Yet another chaotic attactor. *Int. J. Bifurc. Chaos*, 9(7):1465–1466.

[Chen04] G. Chen, Y. Mao, and C. K Chui (2004). A symmetric image encryption based on 3D chaotic maps. *Chaos Soliton Fractals*, 21(3):749–761.

[Cusick99] T.W. Cusick (1999). Gray codes and the symbolic dynamics of quadratic maps. *Electronic Letters*, 35(6):468–469.

[Cvitanović91] P. Cvitanović (1991). Periodic orbits as the skeleton of classical and quantum chaos. *Physica D: Nonlinear Phenomena*, 51(1-3):138–151.

[Daw03] C. S. Daw, C. E. A. Finney, and E. R. Tracy (2003). A review of symbolic analysis of experimental data. *Review of Scientific Instruments*, 74(2):915–930.

[Devaney89] Robert L. Devaney (1989). *Introduction to chaotic dynamical systems*. Addison-Wesley Publishing Company, Inc.

[Ebeling92] W. Ebeling and G. Nicolis (1992). Word frequency and entropy of symbolic sequences: a dynamical perspective. *Chaos, Solitons and Fractals*, 6:635–650.

[Eckmann85] J. P. Eckmann and D. Ruelle (1985). Ergodic theory of chaos and strange attractors. *Rev. Mod. Phys.*, 57(3):617–656.

[Farmer87] J. Doyne Farmer and John J. Sidorowich (1987). Predicting chaotic time series. *Phys. Rev. Lett.*, 59(8):845–848.

[Fernandez08a] V. Fernandez, D. Arroyo, M. J. Garcia, and AB. Orue (2008). Free-space quantum key distribution link at gigahertz clock rates. In *QKD Network Demonstration and Conference*. Viena. URL http://www.secoqc.net/downloads/abstracts/SECOQC-Fernandez.pdf.

[Fernandez08b] V. Fernandez, D. Arroyo, M.J. Garcia, P.A. Hiskett, R.J. Collins, G.S. Buller, and A.B. Orue (2008). Experimental quantum key distribution at a wavelength of $\lambda \approx 850nm$. In L. Hernandez and A. Martin, editors, *X Reunión Española sobre Criptología y Seguridad de la Información (X RECSI)*, pages 157–161, (ISBN 978–84–691–5158–7). Universidad de Salamanca, Salamanca, Spain.

[Gamero97] L. G. Gamero, A. Plastino, and M. E. Torres (1997). Wavelet analysis and nonlinear dynamics in a nonextensive setting. *Physica A: Statistical and Theoretical Physics*, 246(3-4):487 – 509. ISSN 0378-4371.

[Gao08a] Tiegang Gao and Zegqiang Chen (2008). Image encryption based on a new total shuffling algorithm. *Chaos, Solitons and Fractals*, 38(1):213–220.

[Gao08b] Tiegang Gao, Qiaolun Gu, and Zengqiang Chen (2008). A new image encryption algorithm based on hyer-chaos. *Physics Letters A*, 372(4):394–400.

[Gholipour06] A. Gholipour, B. N. Araabi, and C. Lucas (2006). Predicting chaotic time series using neural and neurofuzzy models: A comparative study. *Neural Processing Letters*, 24(3):217–239.

[Goldreich01] Oded Goldreich (2001). *Foundations of cryptography: Volume I Basic Tools*. Cambridge University Press.

[Guan05] Z. H. Guan, F. Huang, and W. Guan (2005). Chaos-based image encryption algorithm. *Phys. Lett. A*, 346(1-3):153–157.

[Guckenheimer79] John Guckenheimer (1979). Sensitive dependence to initial conditions for one dimensional maps. *Communications in Mathematical Physics*, 70(2):133–160.

[Guckenheimer83] John Guckenheimer and Philip Holmes (1983). *Nonlinear Oscillations, Dynamical Systems, and Bifurcations of Vector Fields*. Springer-Verlag.

[Hansen92] K. T. Hansen (1992). Remarks on the symbolic dynamics for the Hénon map. *Physics Letters A*, 165(2):100–104.

[Hao98] Bai-Lin Hao and Wei-Mou Zheng (1998). *Applied symbolic dynamics and chaos*, volume 7. Directions in Chaos,World Scientific.

[Hegger99] R. Hegger, H. Kantz, and T. Schreiber (1999). Practical implementation of nonlinear time series methods: The TISEAN package. *Chaos*, 9(2):413–435.

[Hénon76] M. Hénon (1976). A two-dimensional mapping with a strange attractor. *Communications in Mathematical Physics*, 50(1):69–77.

[Higham61] Nicholas J. Higham (1961). *Accuracy and Stability of Numerical Algorithms*. SIAM, second edition.

[Hilborn00] Robert C. Hilborn (2000). *Chaos and nonlinear dynamics*. Oxford University Press, 2nd edition edition.

[Hirsch74] Morris W. Hirsch and Stephen Smale (1974). *Differential equations, dynamical systems, and linear algebra*. Academic Press, Inc., San Diego, California.

[Huang05] Fangjun Huang and Zhi-Hong Guan (2005). Cryptosystem using chaotic keys. *Chaos, Solitons and Fractals*, 23:851–855.

[Jakimoski01a] G. Jakimoski and L. Kocarev (2001). Analysis of some recently proposed chaos-based encryption algorithms. *Physics Letters A*, 291(6):381–384.

[Jakimoski01b] G. Jakimoski and L. Kocarev (2001). Chaos and Cryptography: Block Encryption Ciphers Based on Chaotic Maps. *IEEE Transactions on Circuits and Systems-I: Fundamental Theory and Applications*, 48(2):163–169.

[Jensen85] Roderick V. Jensen and Christopher R. Myers (1985). Images of the critical point of nonlinear maps. *Physical Review A*, 32(2):1222–1224.

[Kahn96] David Kahn (1996). *The codebreakers*. Scribner.

[Kantz94] H. Kantz (1994). A robust method to estimate the maximal lyapunov exponent of a time series. *Physics Letters A*, 185(1):77–87.

[Keller03] K. Keller and H. Lauffer (2003). Symbolic analysis of high-dimensional time series. *International Journal of Bifurcation and Chaos in Applied Sciences and Engineering*, 13:2657–2668.

[Keller04] Karsten Keller and Katharina Wittfeld (2004). Distances of time series by means of symbolic dynamics. *International Journal of Bifurcation and Chaos*, 14(2):693 – 703.

[Keller05] K. Keller and M. Sinn (2005). Ordinal analysis of time series. *Physica A: Statistical Mechanics and its Applications*, 356:114–120.

[Keller07] K. Keller, M. Sinn, and J. Emons (2007). Time series from the ordinal viewpoint. *Stochastics and Dynamics*, 7:247–272.

[Kennel03] Matthew B. Kennel and Michael Buhl (2003). Estimating good discrete partitions from observed data: Symbolic false nearest neighbors. *Phys. Rev. Lett.*, 91(8):084102.

[Kitchens97] Bruce P. Kitchens (1997). *Symbolic Dynamics: One-Sided, Two-Sided and Countable State Markov Shifts*. Springer.

[Kocarev01a] L. Kocarev (2001). Chaos-based cryptography: A brief overview. *IEEE Circuits and Systems Magazine*, 1(2):6–21.

[Kocarev01b] L. Kocarev and G. Jakimoski (2001). Logistic map as a block encryption algorithm. *Physics Letters A*, 289:199–206.

[Kocarev03] L. Kocarev and Z. Tasev (2003). Public-key encryption based on chebyshev maps. volume 3, pages III28–III31.

[Kocarev04] L. Kocarev, P. Amato, D. Ruggiero, and I. Pedaci (2004). Discrete Lyapunov exponent for Rijndael block cipher. In *NOLTA'04*, pages 609–612.

[Kocarev05] L. Kocarev, J. Makraduli, and P. Amato (2005). Public-key encryption based on chebyshev polynomials. *Circuits, Systems, and Signal Processing*, 24(5 SPEC. ISS.):497–517.

[Kocarev06] L. Kocarev, J. Szczepanski, J.M. Amigo, and I. Tomovski (2006). Discrete chaos-i: Theory. *Circuits and Systems I: Regular Papers, IEEE Transactions on*, 53(6):1300–1309. ISSN 1549-8328.

[Kocher96] Paul C. Kocher (1996). Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems. In Springer Berlin / Heidelberg, editor, *Advances in Cryptology-CRYPTO'96*, volume 1109/1996 of *Lecture Notes in Computer Science*, pages 104–113.

[Kreher98] D. L. Kreher and D. R. Stinson (1998). *Combinatorial Algorithms; Generation, Enumeration & Search*. CRC Press.

[Krieger70] W. Krieger (1970). On entropy and generators of measure-preserving transformations. *Transactions of the American Mathematical Society*, 149:453–464.

[Kurian08] Ajeesh P. Kurian and Sadasivan Puthusserypady (2008). Self-synchronizing chaotic stream ciphers. *Signal Processing*, 88:2442–2452. ISSN 0165-1684.

[Kuznetsov98] Yuri A. Kuznetsov (1998). *Elements of applied bifurcation theory*. Springer-Verlag, New-York, 2nd edition.

[Kwok07] H. S. Kwok and W. K. S. Tang (2007). A fast image encryption system based on chaotic maps with finite precision representation. *Chaos Soliton Fractals*, 32(4):1518–1529.

[Lemarié90] P.G. Lemarié (1990). Les ondelettes. *Lecture Notes in Mathematics no. 1438, Springer-Verlag, Berlin*.

[Letellier08] C. Letellier, I. M. Moroz, and R. Gilmore (2008). Comparison of tests for embeddings. *Physical Review E - Statistical, Nonlinear, and Soft Matter Physics*, 78(2).

[Li03] Shujun Li (2003). *Analyses and New Designs of Digital Chaotic Ciphers*. Ph.D. thesis, School of Electronic and Information Engineering, Xi'an Jiaotong University, Xi'an, China. Available online at http://www.hooklee.com/pub.html.

[Li04a] Shujun Li (2004). When chaos meets computers. URL http://arxiv.org/abs/nlin.CD/0405038, last revised in December 2005.

[Li04b] Shujun Li, Guangrong Chen, Kwok-Wo Wong, Xuanqin Mou, and Yuanlong Cai (2004). Baptista-type chaotic cryptosystems: problems and countermeasures. *Physics Letters A*, 332:368–375.

[Li05a] Shujun Li, Gonzalo Alvarez, and G. Chen (2005). Breaking a chaos-based secure communication scheme designed by an improved modulation method. *Chaos, Solitons & Fractals*, 25(1):109–120.

[Li05b] Shujun Li, Guanrong Chen, and Xuanqin Mou (2005). On the dynamical degradation of digital piecewise linear chaotic maps. *International Journal on Bifurcation and Chaos*, 15(10):3119–3151.

[Li07a] Chengqing Li, Shujun Li, Gonzalo Alvarez, Guanrong Chen, and Kwok-Tung Lo (2007). Cryptanalysis of two chaotic encryption schemes based on circular bit shift and XOR operations. *Physics Letters A*, 369:23–30.

[Li07b] Shujun Li, Gonzalo Alvarez, Zhong Li, and Wolfgang A. Halang (2007). 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*, page 92. A complete edition available online at http://lib.physcon.ru/?item=1368 and http://www.hooklee.com/Papers/PhysCon2007.pdf.

[Li08] Shujun Li, Chengqing Li, Guanrong Chen, Nikolaos G. Bourbakis, and Kwok-Tung Lo (2008). A general quantitative cryptanalysis of permutation-only multimedia ciphers against plaintext attacks. *Signal Processing: Image Communication*, 23(3):212–223.

[Li09] Hengjian Li and Jiashu Zhang (2009). A secure and efficient entropy coding based on arithmetic coding. *Communications in Nonlinear Science and Numerical Simulation*, 14(12):4304 – 4318. ISSN 1007-5704.

[Lind95] Douglas Lind and Brian Marcus (1995). *An Introduction to Symbolic Dynamics and Coding*. Cambridge University Press.

[Ling07] Bingo Wing-Kuen Ling, Charlotte Yuk-Fan Ho, and Peter Kwong-Shun Tam (2007). Chaotic filter bank for computer cryptography. *Chaos, Solitons and Fractals*, 34:817–824.

[Lorenz63] E.N. Lorenz (1963). Deterministic nonperiodic flow. *Journal of the Atmospheric Sciences*, 20:130–141.

[Majtey05] A. P. Majtey, P. W. Lamberti, M. T. Martin, and A. Plastino (2005). Wootters' distance revisited: a new distinguishability criterium. *Eur. Phys. J. D*, 32:413–419.

[Mallat89] S. Mallat (1989). A theory for multiresolution signal decomposition: the wavelet representation. *IEEE Trans. on Patt. Anal. and Mach. Intell.*, 11(7):674–693.

[Mallat99] S. Mallat (1999). *A wavelet tour of signal proccessing*. Academic Press, 2nd edition.

[Mao04] Y. Mao, G. Chen, and S. Lian (2004). A novel fast image encryption scheme based on 3d chaotic baker maps. *International Journal of Bifurcation and Chaos in Applied Sciences and Engineering*, 14(10):3613–3624.

[Martin06] M.T. Martin, A. Plastino, and O.A. Rosso (2006). Generalized statistical complexity measures: Geometrical and analytical properties. *Physica A: Statistical Mechanics and its Applications*, 369(2):439–462.

[Marwan07] Norbert Marwan, M. Carmen Romano, Marco Thiel, and Jürgen Kurths (2007). Recurrence plots for the analysis of complex systems. *Physics Reports*, 438:237–329.

[Masuda01] N. Masuda and K. Aihara (2001). Prediction of chaotic time series with wavelet coefficients. *Electronics and Communications in Japan, Part III: Fundamental Electronic Science (English translation of Denshi Tsushin Gakkai Ronbunshi)*, 84(6):50–59.

[Masuda06] N. Masuda, G. Jakimoski, K. Aihara, and L. Kocarev (2006). Chaotic block ciphers: from theory to practical algorithms. *Circuits and Systems I: Regular Papers, IEEE Transactions on*, 53(6):1341–1352. ISSN 1549-8328.

[May76] Robert May (1976). Simple mathematical models with very complicated dynamics. *Nature*, 261:459 – 467.

[Menezes97] A.J. Menezes, P.C van Oorschot, and S.A. Vanstone (1997). *Handbook of Applied Cryptography*. CRC Press.

[Metropolis73] N. Metropolis, M.L. Stein, and P.R. Stein (1973). On finite limit sets for transformations on the unit interval. *Journal of Combinatorial Theory (A)*, 15:25–44.

[Mi07] Bo Mi, Xiaofeng Liao, and Yong Chen (2007). A novel chaotic encryption scheme based on arithmetic coding. Accepted by Chaos, Solitons and Fractals, In Press, doi:10.1016/j.chaos.2007.01.133.

[Millérioux08] G. Millérioux, J. M. Amigó, and J. Daafouz (2008). A connection between chaotic and conventional cryptography. *IEEE Transactions on Circuits and Systems I: Regular Papers*, 55(6):1695–1703.

[Nagaraj08] N. Nagaraj, M. C. Shastry, and P. G. Vaidya (2008). Increasing average period lengths by switching of robust chaos maps in finite precision. *European Physical Journal: Special Topics*, 165(1):73–83.

[Nagaraj09] N. Nagaraj, P. G. Vaidya, and K. G. Bhat (2009). Arithmetic coding as a non-linear dynamical system. *Communications in Nonlinear Science and Numerical Simulation*, 14(4):1013–1020.

[NIST01] NIST (2001). Nist special publication 800-22. URL http://csrc.nist.gov/rng/rng2.html.

[Orúe08a] A. Orúe, V. Fernandez, Gonzalo Alvarez, G. Pastor, M. Romera, and F. Montoya (2008). Determination of the parameters for a Lorenz system and application to break the security of two-channel chaotic cryptosystems. *Physics Letters A*, 372(34):5588–5592.

[Orúe08b] A. Orúe, V. Fernandez, Gonzalo Alvarez, G. Pastor, M. Romera, F. Montoya, and S. Li (2008). Breaking a sc-cnn-based chaotic masking secure communication system. *International Journal of Bifurcation and Chaos*, 0(0):0.

[Orúe07] A. B. Orúe, Gonzalo Alvarez, David Arroyo, Juana Nunez, and Fausto Montoya (2007). Determinación del valor de los parámetros del sistema de Lorenz y aplicación al criptoanálisis de criptosistemas caóticos. In *NoLineal 2007*, page 85.

[Pareek03] N. K. Pareek, Vinod Patidar, and K. K. Sud (2003). Discrete chaotic cryptography using external key. *Physics Letters A*, 309:75–82.

[Pareek05] N. K. Pareek, Vinod Patidar, and K. K. Sud (2005). Cryptography using multiple one-dimensional chaotic maps. *Communications in Nonlinear Science and Numerical Simulation*, 10:715–723.

[Pareek06a] N. K. Pareek, V. Patidar, and K. Sud (2006). Image encryption using chaotic logistic map. *Image and Vision Computing*, 24(9):926–934.

[Pareek06b] N.K. Pareek, V. Patidar, and K. K. Sud (2006). Image encryption using chaotic logistic map. *Image Vis. Comput.*, 24(9):926–934.

[Pastor97] G. Pastor, M. Romera, and F. Montoya (1997). A revision of the Lyapunov exponent in 1D quadratic maps. *Physica D*, 107:17–22.

[Pastor06] Gerardo Pastor, Miguel Romera, Gonzalo Alvarez, David Arroyo, and Fausto Montoya (2006). Equivalence between subshrubs and chaotic bands in the Mandelbrot set. *Discrete Dynamics in Nature and Society*, 2006:Article ID 70471, 25 pages.

[Pastor07a] Gerardo Pastor, Miguel Romera, Gonzalo Alvarez, David Arroyo, and Fausto Montoya (2007). On periodic and chaotic regions in the Mandelbrot set. *Chaos, Solitons and Fractals*, 32(1):15–25.

[Pastor07b] Gerardo Pastor, Miguel Romera, Gonzalo Alvarez, Juana Nunez, David Arroyo, and Fausto Montoya (2007). Operating with external arguments of Douady and Hubbard. *Discrete Dynamics in Nature and Society*, 2007:Article ID 45920, 17 pages.

[Pastor07c] Gerardo Pastor, Miguel Romera, Gonzalo Alvarez, Juana Nunez, David Arroyo, A. B. Orue, and Fausto Montoya (2007). Medallones de espiral múltiple en el conjunto de Mandelbrot. In *NoLineal 2007*, page 77.

[Pastor07d] Gerardo Pastor, Miguel Romera, Gonzalo Alvarez, Juana Nunez, David Arroyo, A. B. Orue, and Fausto Montoya (2007). Pseudoharmonics and pseudoantiharmonics: a new tool to calculate external arguments of Douady and Hubbard. In *International*

Conference on Dynamical methods and Mathematical modelling, page 27. Valladolid.

[Pastor08] Gerardo Pastor, Miguel Romera, Gonzalo Alvarez, David Arroyo, A. B. Orue, Veronica Fernandez, and Fausto Montoya (2008). Algorithm for external arguments calculation of the nodes of a shrub in the Mandelbrot set. *Fractals*, 16(2):159–168.

[Pastor09] G. Pastor, M. Romera, G. Alvarez, D. Arroyo, A.B. Orue, V. Fernandez, and F. Montoya (2009). A general view of pseudoharmonics and pseudoantiharmonics to calculate external arguments of douady and hubbard. *Applied Mathematics and Computation*, 213(2):484 – 497. ISSN 0096-3003.

[Pecora90] L.M. Pecora and T.L. Carroll (1990). Synchronization in chaotic systems. *Phys. Rev. Lett.*, 64(8):821–824.

[Peitgen92] Heinz-Otto Peitgen, Hartmut Jurgens, and Dietmar Saupe (1992). *Chaos and Fractals*. SpringerVerlag. ISBN 0387202293.

[Pethel06] Shawn D. Pethel, Ned J. Corron, and Erik Bollt (2006). Symbolic dynamics of coupled map lattices. *Physica Review Letters*, 96:034105:1–4.

[Piccardi06] Carlo Piccardi (2006). On parameter estimation of chaotic systems via symbolic time-series analysis. *Chaos*, 16:043115:1–10.

[Pisarchik06] A. N. Pisarchik, N. J. Flores-Carmona, and M. Carpio-Valadez (2006). Encryption and decryption of images with chaotic map lattices. *Chaos*, 16(3):Art. No. 033118.

[Powell79] G E Powell and I C Percival (1979). A spectral entropy method for distinguishing regular and irregular motion of hamiltonian systems. *Journal of Physics A: Mathematical and General*, 12(11):2053–2071.

[Rajagopalan06] Venkatesh Rajagopalan and Asok Ray (2006). Symbolic time series analysis via wavelet-based partitioning. *Signal Processing*, 86:3309–3320.

[Rhouma07] R. Rhouma, S. Meherzi, and S. Belghith (2007). OCML-based colour image encryption. accepted by Chaos Solitons Fractals, in press, doi: 10.1016/j.chaos.2007.07.083.

[Rhouma09] Rhouma Rhouma, David Arroyo, and Safya Belghith (2009). A new color image cryptosystem based on a piecewise linear chaotic map. In *International Multi-Conference on Systems, Signals & Devices, Conference on Power Electrical Systems*. Djerba, Tunisia.

[Romera08] M. Romera, Gonzalo Alvarez, D. Arroyo, A.B. Orue, V. Fernandez, and G. Pastor (2008). Drawing and computing external rays in the multiple-spiral medallions of the Mandelbrot set. *Computers & Graphics*, 32:597–610.

[Rosso01] O.A. Rosso, S. Blanco, J. Yordanova, V. Kolev, A. Figliola, M. Schürmann, and E. Basar (2001). Wavelet entropy: a new tool for ananlysis of short duration brain electrical signals. *Journal of Neuroscience Methods*, 105:65–75.

[Rosso02] Osvaldo A. Rosso and María Liliana Mairal (2002). Characterization of time dynamical evolution of electroencephalographic epileptic records. *Physica A: Statistical Mechanics and its Applications*, 312(3-4):469 – 504.

[Ruggiero04] D. Ruggiero, I. Pedaci, P. Amato, and L. Kocarev (2004). Analysis of the chaotic dynamic of Rijndael block cipher. In *RISP Int. Workshop on Nonlinear Circuit and Signal Processing (NCSP'04)*, pages 77–80.

[Schmitz08] R. Schmitz (2008). Public key cryptography: A dynamical systems perspective. In *SECURWARE'08. Second International Conference on Emerging Security Information, Systems and Technologies*, pages 209–212.

[Schuster95] Heinz Georg Schuster (1995). *Deterministic chaos : an introduction / Heinz Georg Schuster*. VCH ; Distribution, USA and Canada, VCH, Weinheim, Federal Republic of Germany : New York, NY, USA :, 3rd rev. ed. edition. ISBN 3527293159.

[Shannon49] Claude Shannon (1949). Communication theory of secrecy systems. *Bell Sys. Tech. J.*, 28:656–715.

[Singh00] Simon Singh (2000). *The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography*. Anchor. ISBN 0-385-49531-5.

[Skrobek08] Adrian Skrobek (2008). Approximation of a chaotic orbit as a cryptanalytical method on Baptista's cipher. *Physics Letters A*, 372(6):849–859.

[Stamp07] Mark Stamp and Richard M. Low (2007). *Applied cryptanalysis: breaking ciphers in the real world*. John Wiley & Sons, Inc., Hoboken, New Jersey, USA.

[Steuer01] R. Steuer, L. Molgedey, W. Ebeling, and M.A. Jiménez-Monta no (2001). Entropy and optimal partition for data analysis. *The European Physical Journal B*, 19:265–269.

[Stinson95] D.R. Stinson (1995). *Cryptography: Theory and Practice*. CRC Press.

[Stojanovski97] T. Stojanovski, L. Kocarev, and R. Harris (1997). Applications of symbolic dynamics in chaos synchronization. *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, 44(10):1014–1018.

[Szczepanski05] J. Szczepanski, J. Amigo, T. Michalek, and L. Kocarev (2005). Cryptographically secure substitutions based on the approximation of mixing maps. *IEEE Transactions on Circuits and Systems-I*, 52:443–453.

[Takens81] F. Takens (1981). Detecting strange attractors in turbulence. *Dynamical Systems and Turbulence, Lecture Notes in Mathematics*, 898:366–381.

[Tang03] Guoning Tang, Shihong Wang, and Huaping Lü (2003). Chaos-based cryptograph incorporated with s-box algebraic operation. *Physics Letters A*, 318:388–398.

[Torres00] M. E. Torres and L. G. Gamero (2000). Relative complexity changes in time series using information measures. *Physica A*, 286:457–473.

[Tsallis88] C. Tsallis (1988). Possible generalization of Boltzmann-Gibbs statistics. *Journal of Statistical Physics*, 52(1-2):479–487.

[Tsonis07] A. A. Tsonis (2007). Reconstructing dynamics from observables: The issue of the delay parameter revisited. *International Journal of Bifurcation and Chaos*, 17(12):4229–4243.

[Udaltsov03] Vladimir S. Udaltsov, Jean-Pierre Goedgebuer, Laurent Larger, Jean-Baptiste Cuenot, Pascal Levy, and William T. Rhodes (2003). Cracking chaos-based encryption systems ruled by nonlinear time delay differential equations. *Physics Letters A*, 308:54–60.

[Vernam25] Gilbert Vernam (1925). Cipher printing telegraph systems for secret wire and radio telegraphic communications. *Journal of the IEEE*, 5:109–115.

[Walters82] Peter Walters (1982). *An Introduction to Ergodic Theory*, volume 79 of *Graduate Texts in Mathematics*. Springer-Verlag, New York.

[Wang87] Li Wang and Nicholas D. Kazarinoff (1987). On the universal sequence generated by a class of unimodal functions. *Journal of Combinatorial Theory, Series A*, 46:39–49.

[Wang05] Kai Wang, Wenjiang Pei, Liuhua Zou, Aiguo Song, and Zhenya He (2005). On the security of 3d cat map based on symmetric image encryption scheme. *Physics Letters A*, 343:432–439.

[Wang07] Yong Wang, Xiaofeng Liao, Tao Xiang, Kwok-Wo Wong, and Degang Yang (2007). Cryptanalysis and improvement on a block cryptosystem based on iteration a chaotic map. *Physics Letters A*, 363:277–281.

[Wang08a] Kai Wang, Wengjiang Pei, Shaoping Wang, Yiu-Ming Cheung, and Zhenya He (2008). Symbolic vector dynamics approach to initial condition and control parameters estimation of coupled map lattices. *IEEE Transactions on Circuits and Systems-I: Regular Papers*, 55:1116–1124.

[Wang08b] Xing-yuan Wang and Qing Yu (2008). A block encryption algorithm based on dynamic sequences of multiple chaotic systems.

Communications in Nonlinear Science and Numerical Simulation. In Press.

[Wang08c] Xingyuan Wang, Chaofeng Duan, and Nini Gu (2008). A new chaotic cryptography based on ergodicity. *International Journal of Modern Physics B*, 22(7):901–908.

[Wang08d] Yong Wang, Kwok-Wo Wong, Xiaofeng Liao, Tao Xiang, and Guanrong Chen (2008). A chaos-based image encryption algorithm with variable control parameters. *Chaos, Solitons & Fractals*, In Press, Corrected Proof:–. ISSN 0960-0779.

[Wei06a] Jun Wei, Xiaofeng Liao, K.W. Wong, Tsing Zhou, and Yigui Deng (2006). Analysis and improvement for the performance of baptista's cryptographic scheme. *Physics Letters A*, 354:101–109.

[Wei06b] Jun Wei, Xiaofeng Liao, Kwok-wo Wong, and Tao Xiang (2006). A new chaotic cryptosystem. *Chaos, Solitons and Fractals*, 30:1143–1152.

[Wong01] W. Wong, L. Lee, and K. Wong (2001). A modified chaotic cryptographic method. *Comput. Phys. Comm.*, 138:234–236.

[Wong02] K. W. Wong (2002). A fast chaotic cryptographic scheme with dynamic look-up table. *Physics Letters A*, 298:238–242.

[Wong03] K. W. Wong (2003). A combined chaotic cryptographic and hashing scheme. *Physics Letters A*, 307:292–298.

[Wong08] Kwok-Wo Wong, Bernie Sin-Hung Kwok, and Wing-Shing Law (2008). A fast image encryption scheme based on chaotic standard map. *Physics Letters A*, 372(15):2645–2652.

[Wu04] Xiaogang Wu, Hanping Hu, and Baoliang Zhang (2004). Parameter estimation only from the symbolic sequences generated by chaos system. *Chaos, solitons and Fractals*, 22:359–366.

[Xiang06] Tao Xiang, Xiaofeng Liao, Guoping Tang, Yong Chen, and Kwok wo Wong (2006). A novel block cryptosystem based on iterating a chaotic map. *Physics Letters A*, 349:109–115.

[Xiang07] Tao Xiang, Shihong Wang, Huaping Lü, and Gang Hu (2007). A novel symmetrical cryptosystem based on discretized two-dimensional chaotic map. *Physics Letters A*, 364:252–258.

[Yang08] Huaqian Yang, Xiaofeng Lia, Kwok wo Wong, Wei Zhang, and Pengcheng Wei (2008). A new cryptosystem based on chaotic map and operations algebraic. Accepted by Chaos, Solitons and Fractals, In Press, doi:10.1016/j.chaos.2007.10.046.

Index