Chaotic Cryptosystems: Cryptanalysis and Identifiability

Floriane Anstett, Gilles Millérioux, Gérard Bloch

Chaotic Cryptosystems: Cryptanalysis and Identifiability

Floriane Anstett, Gilles Millerioux and Gérard Bloch*

Abstract

A general framework and a systematic methodology for the cryptanalysis of a large class of chaotic cryptosystems are proposed. More precisely, it is tested, a priori, during the design stage, whether the parameters of a chaotic cryptosystem may play the role of the secret key or not. Robustness against brute force attacks is first considered. A connection between uniqueness in the parameters and identifiability is pointed out. Two approaches, the outputs equality approach and the input/output relation approach, are presented to test the identifiability of the system parameters. The second approach is constructive in the sense that not only it allows to conclude on the identifiability of the parameters but it also provides a systematic technique to retrieve the parameters in the context of a known plaintext attack. It is shown that cryptosystems involving polynomial nonlinearities, chaotic or not, are weak against this attack, called algebraic attack.

Keywords: Chaotic cryptosystems, cryptanalysis, identifiability, brute force attack, known plaintext attack, algebraic attack

1 Introduction

Chaotic behavior is one of the most complex dynamics a nonlinear system can exhibit. Because the signals resulting from chaotic systems are broadband, noiselike, difficult to predict, the idea of using chaotic systems for information masking has received much attention since the pioneering work of [1]. The proposed communication schemes involve a chaotic transmitter system and a receiver system. The transmitter input is the information to be masked, the plaintext, and its output is the encrypted information, the ciphertext, conveyed to the receiver. Several methods for "hiding" an information signal into a chaotic signal have been proposed in the literature. An overview can be found according to the chronology in [2][3][4][5] including the chaotic masking, the chaotic switching, the parameter modulation, the message embedding. These methods are defined either for continuous-time or discrete-time systems. In general, the decryption mechanism requires the synchronization between the transmitter and the receiver.

An essential issue for the validation of cryptosystems is the cryptanalysis, that is the study of attacks against cryptographic schemes in order to reveal their possible weakness. A fundamental assumption in cryptanalysis, first stated by A. Kerkhoff in 1883 [6], is that the adversary knows all the details of the cryptosystem, including the algorithm and its implementation, except the secret key, on which the security of the cryptosystem must be entirely based. As for chaotic cryptosystems, the system parameters play a central role because they are expected to act as the secret key.

One of the problems of great importance related to this issue is the parameters recovering. In the related literature, the Kerkhoff assumption is formulated and a known plaintext attack, where an information sequence (plaintext) and the corresponding output sequence (ciphertext) are known, is considered. In [7] [8] [9] and [10], the parametric cryptanalysis of different usual schemes based on chaotic systems (Lorenz, Rössler, ...) is proposed. It is shown that the considered encryption schemes are not sufficiently sensitive to parameter

*The authors are with the Centre de Recherche en Automatique de Nancy, Nancy Universities, CRAN - ESSTIN, 2 Rue Jean Lamour 54519 Vandoeuvre Les Nancy Cedex, France. Emails: floriane.anstett@esstin.uhp-nancy.fr, gilles.millerioux@esstin.uhp-nancy.fr, gerard.bloch@esstin.uhp-nancy.fr

mismatch. In fact, synchronization for decryption can be achieved despite the parameter mismatch. This reduces the set of all possible key values and reducing this key space increases the chance for the adversary to find the actual key value. The proposed "error function attack" consists in trying a key in the reduced key space and in computing the difference between the output of the actual system and the output of the candidate system, both of them being forced by the same plaintext. If the difference converges to zero, the actual key is recovered. The reconstruction of the system parameters can be refined by resorting to adaptive techniques [11] [12] [13] [14] [15] [16]. The basic idea is to adaptively adjust the parameters to achieve synchronization with remote chaotic systems. A somewhat different method can be found in [17] [18] where a chosen ciphertext attack is considered. For such an attack, the adversary is assumed to control the input of the receiver, the ciphertext, and to analyze the corresponding plaintext sequence. It is shown that the parameters can be reconstructed by solving a set of algebraic equations. Finally, in [19], another approach for the parameter recovering has been investigated for an encryption scheme involving a Lorenz system. The chaotic system is transformed, by eliminating the state variables, into a system depending only on the information, the output, their derivatives and the parameters. The resulting system is solved in the parameters. This approach has been also applied to a chaotic cryptosystem based on the Henon map, in [20] and has been extended to a class of chaotic discrete-time systems in [21]. In this case, the derivatives are replaced by the iterates.

All these works deal with some identification techniques for reconstructing the parameters and most often on some special cases. In this paper, we propose a general framework and a systematic methodology for the cryptanalysis of a large class of chaotic cryptosystems. More precisely, it is tested, a priori, whether the parameters of a chaotic cryptosystem may play the role of the secret key or not. A connection between uniqueness in the secret parameters and identifiability is pointed out. Very few works have established this connection, except for the study in [23]. Some preliminary results have been presented in [24]. Unlike most of the studies encountered in the literature, the proposed test applies during the design stage. Besides, the methodology provided in this paper is independent of the approach one may resort to reconstruct the parameters (adaptive, ...).

The paper is organized as follows. In Section 2, a connection between uniqueness in the secret parameters and identifiability is pointed out. Two approaches, the outputs equality approach and the input/output relation approach, are presented to test the identifiability of the system parameters. Then, in Section 3, a cryptanalytic procedure, based on the identifiability concept, is carried out on some specific examples. It is shown that cryptosystems with polynomial nonlinearities are unfortunately weak against known plaintext attacks. Throughout the manuscript, we only consider discrete-time systems but the results still hold in the continuous case.

2 Problem statement and Identifiability

2.1 Problem statement

Among the different usual methods for hiding an information, additive masking, chaotic switching, parameter modulation, message embedding, we focuse on the last one because all the results given here can be easily transposed to the others.

We recall the message embedding scheme, in the discrete-time case, which involves the transmitter system Σ_θ given by the general form:

$$\Sigma_\theta \left\{ \begin{array}{lcl} x_{k+1} & = & f_\theta(x_k, m_k) \\ y_k & = & h_\theta(x_k, [m_k]) \end{array} \right. \quad (1)$$

where $x_k \in \mathscr{X} \subset \mathbb{R}^n$ is the state vector, $y_k \in \mathscr{Y} \subset \mathbb{R}$ the measured, and so available, output, $m_k \in \mathscr{M} \subset \mathbb{R}$ the information signal, f_θ is a nonlinear chaotic function and h_θ a (possibly) nonlinear function, both parameterized by θ, $\theta = [\theta^{(1)}, \ldots, \theta^{(L)}]^T \in \Theta \subset \mathbb{R}^L$, the parameter vector. The most common nonlinearities f_θ are of polynomial type (Henon map [25], Logistic map [26], Mandelbrot map [27], Arnold's cat map [28], ...). $[m_k]$ means that h_θ can depend on m_k but not necessary. The initial condition of x_k will be denoted x_0. At the receiver side, the information recovering requires a synchronization mechanism. Details of chaos-based synchronization are

described in [29] [30].
Having in mind the encryption purposes, we only consider the practical case where the system Σ_θ has a single input m_k and a single output y_k but the following results can be extended to the case of multiple inputs and multiple outputs.
We assume that the cryptosystem must face the most basic attack, i.e. the brute force attack. This attack consists in trying exhaustively every possible parameter value in the parameter space (which is in practice a finite space), in order to retrieve the secret key [31]. The brute force attack is the most expensive one, owing to the exhaustive search. The quicker the brute force attack succeeds, the weaker the cryptosystem is. The worst situation for the eavesdropper, and the best for the security, is that there exists a unique solution. In this case, the probability of finding the actual parameter value is the lowest. The key idea is that the uniqueness of the parameters is directly linked to the parametric identifiability concept [32]. Some basic backgrounds are recalled below.

2.2 Identifiability

The following definitions are borrowed from [33].

Definition 1 *An input sequence over a window of iterations $[0-T]$, denoted by $\{m_k\}_0^T$, is called an* admissible input on $[0-T]$ *if the difference equation (1) admits a unique local solution.*

Definition 2 *The system Σ_θ is* locally strongly x_0-identifiable *at θ through the admissible input sequence $\{m_k\}_0^T$ if there exists an open neighborhood of θ, $v(\theta) \subset \Theta$, such that for any $\hat{\theta} \in v(\theta)$ and for any $\theta \in v(\theta)$:*

$$\hat{\theta} \neq \theta \quad \Rightarrow \quad \{y_k(x_0, m_k, \hat{\theta})\}_0^T \neq \{y_k(x_0, m_k, \theta)\}_0^T \tag{2}$$

Definition 3 *The system Σ_θ is* structurally identifiable *if there exist $T > 0$, an open subset $\mathscr{X}_0 \subset \mathscr{X}$ and some dense subsets $v(\theta) \subset \Theta$ and $\mathscr{M}_0^T \subset \mathscr{M}$, such that, for every $x_0 \in \mathscr{X}_0$, $\theta \in v(\theta)$ and $\{m_k\}_0^T \in \mathscr{M}_0^T$, the system Σ_θ is locally strongly x_0-identifiable at θ through the admissible input sequence $\{m_k\}_0^T$.*

In the following, we will equally say that the system or its parameters are structurally identifiable.

Remark 1 *In the definitions above, the subset $\mathscr{X}_0$ is open in order to avoid considering an atypical set of zero measure which leads to singularities and where no conclusion about identifiability is possible. Moreover, these definitions are given for the initial condition taken at the particular time step $k = 0$. However, we can consider any time step k because the system (1) is shift-invariant.*

Remark 2 *The Definition 3 is a direct discrete-time counterpart of that of the structural identifiability of continuous-time systems, given in [34] and is equivalent to the definition of rational identifiability of [35].*

To test the identifiability of system parameters, two approaches, the outputs equality approach and the input/output relation approach can be performed.

2.3 Outputs Equality Approach

The outputs equality approach is directly based on Definition 3. The trajectories $y_k(\theta)$ contain information about the unknown parameter vector θ. The approach consists in testing whether the equality of the output trajectories of systems Σ_θ and $\Sigma_{\hat{\theta}}$, over an iteration window $[0-T]$, implies the equality of the parameter vectors θ and $\hat{\theta}$. So, the following theorem states a *sufficient condition* for structural identifiability of system (1).

Theorem 1 *The system Σ_θ (1) is structurally identifiable if the set of equations:*

$$\{y_k(x_0, m_k, \hat{\theta})\}_0^T = \{y_k(x_0, m_k, \theta)\}_0^T \tag{3}$$

has a unique solution for $\hat{\theta}$, that is $\hat{\theta} = \theta$.

The proof is a direct consequence of the implication (2).

Remark 3 *In the case of continuous-time systems, this approach is formulated as the Taylor series expansion approach [36]. To test their equality, the output trajectories are approximated by their Taylor series expansions, whose coefficients are unique and contain information about the parameters. The aim is then to test whether the equality of the coefficients of the Taylor series expansions implies the equality of the parameter vectors θ and $\hat{\theta}$ or not.*

Remark 4 *T is a positive integer and represents the number of iterations required to prove that (3) $\Rightarrow \hat{\theta} = \theta$. If T goes to infinity and the previous relation cannot be proved, no conclusion on structural identifiability can be given. As T is unknown a priori, Theorem 1 is only a sufficient condition of structural identifiability.*

Besides, to recover θ, Theorem 1 requires the knowledge of the initial condition. Actually, to test the structural identifiability, there exists another method which is independent of the initial condition : the input/output relation approach, detailed in the next section.

2.4 Input/Output Relation Approach

The following theorem is a discrete-time counterpart of the theorem given in [34] for continuous-time systems. It formulates a *necessary and sufficient condition* for the parametric structural identifiability.

Theorem 2 *The system Σ_θ (1) is structurally identifiable if and only if there exists two integers $N < \infty$ and $N^{'} < \infty$ such that the equations (1) can be rearranged in a linear regression such that, for $i = 1, \ldots, L$ (L is the dimension of the parameter vector):*

$$\begin{array}{l} P_i(y_k, \ldots, y_{k+N}, m_k, \ldots, m_{k+N'})\theta^{(i)} \\ -Q_i(y_k, \ldots, y_{k+N}, m_k, \ldots, m_{k+N'}) = 0 \end{array} \quad (4)$$

where P_i and Q_i are functions depending only on y_k, m_k and on their iterates.

If Theorem 2 holds, it is clear that every parameter $\theta^{(i)}$ can be written as:

$$\theta^{(i)} = \frac{Q_i(y_k, \ldots, y_{k+N}, m_k, \ldots, m_{k+N'})}{P_i(y_k, \ldots, y_{k+N}, m_k, \ldots, m_{k+N'})} \quad (5)$$

unless P_i vanishes. The condition $P_i \neq 0$ is called the *persistent excitation (PE) condition*. The set of values of y_k and m_k corresponding to $P_i = 0$ is a set of zero measure, in general. This set of zero measure is omitted because we only consider the set of admissible inputs (Definition 1).

To obtain (4), we must first eliminate the variable x_k and its iterates in (1), considered as indeterminates. That leads to a relation depending only on the parameter vector θ, the output y_k, the input m_k and their iterates, called the input/output relation:

$$\mathscr{L}_1(\theta, y_k, \ldots, y_{k+s}, m_k, \ldots, m_{k+s'}) = 0 \quad (6)$$

where s is the observability index of the system (1) [37] and $s^{'} \leq s$.

Important remarks: It is worth pointing out that this approach is constructive. It allows not only to conclude on the parameter identifiability but also provides a way for retrieving the parameters in the context of a known plaintext attack. Indeed, regarding (5), both the input and the output must be known.
For chaotic cryptosystems involving polynomial nonlinearities, the functions P_i and Q_i in (4) are polynomials and (5) can be easily obtained. As a result, the chaotic cryptosystems involving polynomial nonlinearities can be always easily broken and that reveals their weakness. The corresponding attack is called a known plaintext algebraic attack.

In the following, two approaches for the state elimination, the Gröbner bases approach and the characteristic set approach, dedicated to polynomial nonlinearities, are presented.

2.4.1 Gröbner bases approach

The method of the Gröbner bases is borrowed from the algebra. The first algorithm of this type is due to [38]

and has been first applied for identifiability purposes by [34] in the case of continuous-time systems. Some notions of differential algebra can be found in [39] for continuous-time systems. However, they can equally be defined with the derivative operator (continuous-time case) or with the delay operator (discrete-time case). Some recalls in the case of discrete-time systems are carried out below.

Consider a system Σ_θ of the polynomial ring, denoted by $\mathbb{A} = \mathbb{R}[x_k^{(1)}, \ldots, x_k^{(n)}]$ where the indeterminates are the state vector components, $x_k^{(1)}, \ldots, x_k^{(n)}$, and the coefficients are real numbers.

Definition 4 *An* ideal *of* $\mathbb{A}$ *is a subset* I *of* $\mathbb{A}$*, such that, for polynomials* p *and* q*:*

- $\forall p \in I$, $\forall q \in I$, $p+q \in I$,
- $\forall p \in I$, $\forall g \in \mathbb{A}$, $pg \in I$

For the system Σ_θ (1) with polynomial nonlinearities, the ideal $I \subset \mathbb{A}$ is the set of all the linear combinations of equations (1) and their iterates.

Definition 5 *A* lexicographic order *is a ranking according to the names of the variables and their iterates such that:*

- $x_k^{(i)} < x_{k+l}^{(i)}$, $\forall l \in \mathbb{N}$,
- $x_m^{(i)} < x_l^{(j)} \Rightarrow x_{m+t}^{(i)} < x_{l+t}^{(j)}$, $\forall m \in \mathbb{N}$, $\forall l \in \mathbb{N}$, $\forall t \in \mathbb{N}$,
- $x_k^{(i)} < x_k^{(j)} \Rightarrow (x_k^{(i)})^\alpha < (x_k^{(j)})^\beta$, $\forall \alpha \in \mathbb{N}$, $\forall \beta \in \mathbb{N}$

To obtain (6), the variables of (1) to be eliminated are considered as the greatest.

If a given pair (m_k, y_k) satisfies (1), it will also satisfy the equations obtained by addition, multiplication and iteration of (1), that are the equations of the ideal associated to (1). For a given lexicographic order, it then suffices to find a basis of this ideal such that one expression of the basis does no longer contain the variables x_k, but only y_k, m_k, their iterates and θ. This expression is of the form (6). Such a basis is called a *Gröbner basis*. A more formal definition of the Gröbner bases can be found in [38] and a theorem of variable elimination based on this method is detailed in [40].

Another way of eliminating the state vector x_k in (1) to obtain the relation (6) is called the characteristic set approach and is detailed in the next section.

2.4.2 Characteristic set approach

The theory of the characteristic set was introduced by Ritt [41]. Before explaining what is a characteristic set, the following definitions are required.

Definition 6 *Given a lexicographic order and a polynomial* $p \in \mathbb{A}$*, the* leader *of the polynomial* p *is the highest ranked iterate of the variables appearing in* p*.*

Definition 7 *A polynomial* A_i *is* reduced *with respect to a polynomial* A_j *if* A_i *contains neither the leader of* A_j *with equal or greater algebraic degree, nor its iterates. A set of polynomials* $A = \{A_1, \ldots, A_i\}$ *that are all reduced with respect to each other is called an* autoreduced set*.*

Two autoreduced sets, $A = \{A_1, A_2, \ldots, A_r\}$ and $B = \{B_1, B_2, \ldots, B_m\}$, ordered in increasing rank with respect to their leaders so that $A_1 < A_2 < \ldots < A_r$, $B_1 < B_2 < \ldots < B_m$, are ranked according to the following principle:

- If there exists an integer l, $l \leq min(r,m)$ such that rank(A_i)=rank(B_i) for $i = 1, \ldots, l-1$ and rank(A_l)<rank(B_l), then A is of lower rank than B.
- If $r < m$ and rank(A_i)=rank(B_i) for $i = 1, \ldots, r$, then A is also of lower rank than B.

Definition 8 *A lowest rank autoreduced set that can be formed with polynomials belonging to a given set of*

polynomials is called a characteristic set.

The characteristic set of system (1) is of the triangular form:

$$\begin{aligned}
&A_1(y_k,\ldots,y_{k+s},m_k,\ldots,m_{k+s'},\theta^{(1)},\ldots,\theta^{(L)})=0\\
&A_2(y_k,\ldots,y_{k+s},m_k,\ldots,m_{k+s'},\theta^{(1)},\ldots,\theta^{(L)},x_k^{(1)})=0\\
&\vdots\\
&A_{n+1}(y_k,\ldots,y_{k+s},m_k,\ldots,m_{k+s'},\theta^{(1)},\ldots,\theta^{(L)},x_k^{(1)},\ldots,x_k^{(n)})\\
&=0
\end{aligned} \tag{7}$$

The relation $A_1 = 0$ represents the input/output relation (6).

Note that each component $x_k^{(i)}$ of the state vector can also be expressed from $\{A_2,\ldots,A_{n+1}\}$, as a function only depending on the input, the output, their iterates and the parameters. This is due to the triangular form of (7). So, the initial condition x_k can be deduced from $\{A_2,\ldots,A_{n+1}\}$.

2.4.3 Summary

The proposed method is summed up by the following steps.

- The system (1) is iterated s times, where s is the observability index of system (1). Usually, s is equal to the dimension n of the system.
- The Gröbner bases or the characteristic set associated to the system (1) and its iterates is computed in order to obtain the input/output relation (6). This can be achieved with symbolic computation software (Maxima, Maple, ...).
- The input/output relation (6) is iterated up to the dimension L of the parameter vector, in order to get as much equations as unknowns:

$$\begin{aligned}
&\mathscr{L}_1(\theta,y_k,\ldots,y_{k+s},m_k,\ldots,m_{k+s'})=0\\
&\vdots\\
&\mathscr{L}_L(\theta,y_{k+L-1},\ldots,y_{k+N},m_{k+L-1},\ldots,m_{k+N'})=0
\end{aligned} \tag{8}$$

  where N is $s+L-1$ and $N' \leq N$.

- From (8), we check if the relations (4) or equivalently (5) can be obtained for every parameter.

The proposed method can be extended for the continuous-time systems. In this case, we consider the derivatives instead of the iterates.

3 Parametric cryptanalysis

In this section, the parametric cryptanalysis of usual chaotic discrete-time cryptosystems involving polynomial nonlinearities is carried out through the concept of identifiability. The context, given at the beginning of the paper, is briefly recalled.
It is tested, a priori, during the design stage, whether the parameters of a chaotic cryptosystem may play the role of the secret key or not. It is assumed that the eavesdropper is supposed to know the structure of the system and the signal y_k, as usual in cryptography [6]. It is tested whether the cryptosystem to be designed is able to face two kinds of attacks.

The first attack to face is the brute force attack which consists in trying exhaustively every possible value for the parameters. For assessing the security in this context, we check if the parameters are identifiable, i.e. a given input/output behavior corresponds to a unique value for the parameters. This situation is the best for the security of the cryptosystem as previously pointed out.
The second attack to face is the known plaintext attack where the eavesdropper chooses a sequence $\{m_k\}$ and analyzes the corresponding sequence $\{y_k\}$. For assessing the security in this context, we check if the parameters can be easily recovered by the input/output relation approach. This approach corresponds to an algebraic attack.
These distinct attacks along with the two approaches, namely, the outputs equality approach and the input/output relation approach, are illustrated through two examples.

3.1 Example 1

Consider the message embedding scheme (1) where the information m_k is embedded in the Henon map [25]:

$$\left\{\begin{array}{lcl} x_{k+1}^{(1)} & = & \theta^{(1)}(x_k^{(1)})^2+\theta^{(2)}x_k^{(2)}+m_k \\ x_{k+1}^{(2)} & = & \theta^{(3)}x_k^{(1)}+\theta^{(4)}m_k \\ y_k & = & x_k^{(1)} \end{array}\right. \quad (9)$$

In this example, the structural identifiability of the parameter vector $[\theta^{(1)} \quad \theta^{(2)} \quad \theta^{(3)} \quad \theta^{(4)}]^T$ ($L=4$) is only treated through the input/output relation approach where the state is eliminated with the Gröbner bases approach.
Since $x_k^{(2)}$ is not directly transmitted through the signal y_k, it is chosen to be the greatest and the corresponding lexicographic order is:

$$x_k^{(1)} < x_{k+1}^{(1)} < x_{k+2}^{(1)} < x_k^{(2)} < x_{k+1}^{(2)} < x_{k+2}^{(2)} \quad (10)$$

It can be shown that the observability index of system (9) is equal to the dimension of the system, $n=2$.
For obtaining the input/output relation, that is $\mathscr{L}_1=0$, the system (9) is first iterated twice:

$$\left\{\begin{array}{l} x_{k+1}^{(1)}-\theta^{(1)}(x_k^{(1)})^2-\theta^{(2)}x_k^{(2)}-m_k=0 \\ x_{k+2}^{(1)}-\theta^{(1)}(x_{k+1}^{(1)})^2-\theta^{(2)}x_{k+1}^{(2)}-m_{k+1}=0 \\ x_{k+1}^{(2)}-\theta^{(3)}x_k^{(1)}-\theta^{(4)}m_k=0 \\ x_{k+2}^{(2)}-\theta^{(3)}x_{k+1}^{(1)}-\theta^{(4)}m_{k+1}=0 \\ y_k-x_k^{(1)}=0 \\ y_{k+1}-x_{k+1}^{(1)}=0 \\ y_{k+2}-x_{k+2}^{(1)}=0 \end{array}\right. \quad (11)$$

The software Maxima, available for free at `http://maxima.sourceforge.net`, computes, with the function `poly_buchberger`, the Gröbner basis of the ideal associated to system (11), with the lexicographic order (10). One of the Gröbner basis expressions is the input/output relation (6):

$$\theta^{(1)}y_{k+1}^2+\theta^{(2)}\theta^{(3)}y_k-y_{k+2}+m_{k+1}+\theta^{(2)}\theta^{(4)}m_k=0 \quad (12)$$

The others expressions of the basis are useless for our purpose since they involve the state vector. Then, the input/output relation (12) is iterated $L-1=3$ times and yields $\mathscr{L}_2=0$, $\mathscr{L}_3=0$ and $\mathscr{L}_4=0$, respectively:

$$\begin{array}{l} \theta^{(1)}y_{k+2}^2+\theta^{(2)}\theta^{(3)}y_{k+1}-y_{k+3}+m_{k+2}+\theta^{(2)}\theta^{(4)}m_{k+1}=0 \\ \theta^{(1)}y_{k+3}^2+\theta^{(2)}\theta^{(3)}y_{k+2}-y_{k+4}+m_{k+3}+\theta^{(2)}\theta^{(4)}m_{k+2}=0 \\ \theta^{(1)}y_{k+4}^2+\theta^{(2)}\theta^{(3)}y_{k+3}-y_{k+5}+m_{k+4}+\theta^{(2)}\theta^{(4)}m_{k+3}=0 \end{array} \quad (13)$$

From the set of equations (12) and (13), it can be shown, for example by using the function `solve` of Maxima, that the relation (4) is only fulfilled for $\theta^{(1)}$:

$$\begin{array}{l} P_1(y_k,\ldots,y_{k+5},m_k,\ldots,m_{k+4})\theta^{(1)} \\ -Q_1(y_k,\ldots,y_{k+5},m_k,\ldots,m_{k+4})=0 \end{array} \quad (14)$$

with:

$$\begin{array}{l} P_1(y_k,\ldots,y_{k+5},m_k,\ldots,m_{k+4})= \\ -m_ky_{k+1}y_{k+3}^2+m_{k+1}y_ky_{k+3}^2+m_ky_{k+2}^3-m_{k+2}y_ky_{k+2}^2 \\ -m_{k+1}y_{k+1}^2y_{k+2}+m_{k+2}y_{k+1}^3 \end{array}$$

$$\begin{array}{l} Q_1(y_k,\ldots,y_{k+5},m_k,\ldots,m_{k+4})= \\ -(y_{k+1}(m_k(y_{k+4}-m_{k+3})+m_{k+1}m_{k+2}) \\ +y_k(m_{k+1}(m_{k+3}-y_{k+4})+m_{k+2}y_{k+3}-m_{+2}^2) \\ +y_{k+2}(m_k(m_{k+2}-y_{k+3})-m_{k+2}y_{k+1}-m_{k+1}^2)+m_{k+1}y_{k+2}^2) \end{array} \quad (15)$$

So, only $\theta^{(1)}$ is identifiable and thus could play the role of the secret key in the context of brute force attack. At the opposite, since there exist at least numerous pairs ($\theta^{(2)}$, $\theta^{(3)}$) or ($\theta^{(2)}$, $\theta^{(4)}$) verifying the relations (12) and (13), the parameters $\theta^{(2)}$, $\theta^{(3)}$ and $\theta^{(4)}$ are unidentifiable and cannot play the role of the secret key.
As stressed in the important remarks in Section 2.4, according to (5) and here (14), it is clear that, performing a known plaintext attack, the parameter $\theta^{(1)}$ can be easily reconstructed with P_1 and Q_1 in (15). Hence, $\theta^{(1)}$ cannot finally play the role of the secret key.
As a result, this cryptosystem will be weak against a known plaintext attack.

3.2 Example 2

Consider the message embedding scheme (1) where the information m_k is embedded in the Burgers map [42]:

$$\left\{\begin{array}{lcl} x_{k+1}^{(1)} & = & (1+\theta^{(1)})x_k^{(1)}+x_k^{(1)}x_k^{(2)}+m_k \\ x_{k+1}^{(2)} & = & (1-\theta^{(2)})x_k^{(2)}-(x_k^{(1)})^2m_k \\ y_k & = & x_k^{(1)} \end{array}\right. \quad (16)$$

The initial condition is $x_0 = [x_0^{(1)} \quad x_0^{(2)}]^T$.
In the following, the structural identifiability of the parameter vector $[\theta^{(1)} \quad \theta^{(2)}]^T$ ($L = 2$) is tested respectively with the outputs equality and the input/output relation approach.

3.2.1 Outputs Equality Approach

The values of the output trajectory $\{y_k(x_0, m_k, \theta)\}_0^T$ are denoted for short by $y_k(\theta)$. One has:

$$\begin{aligned}
y_0(\theta) &= x_0^{(1)} \\
y_1(\theta) &= (1+\theta^{(1)})x_0^{(1)} + x_0^{(1)}x_0^{(2)} + m_0 \\
y_2(\theta) &= (1+\theta^{(1)})((1+\theta^{(1)})x_0^{(1)} + x_0^{(1)}x_0^{(2)} + m_0) \\
&\quad +((1-\theta^{(2)})x_0^{(2)} - (x_0^{(1)})^2 m_0)((1+\theta^{(1)})x_0^{(1)} \\
&\quad +x_0^{(1)}x_0^{(2)} + m_0) + m_1
\end{aligned} \tag{17}$$

The condition (3) gives here:

$$y_0(\hat{\theta}) = y_0(\theta) \quad \Rightarrow \quad x_0^{(1)} = x_0^{(1)} \tag{18}$$

$$y_1(\hat{\theta}) = y_1(\theta) \quad \Rightarrow \quad (\hat{\theta}^{(1)} - \theta^{(1)})x_0^{(1)} = 0 \tag{19}$$

$$\begin{aligned}
y_2(\hat{\theta}) = y_2(\theta) \Rightarrow \quad & ((\hat{\theta}^{(1)})^2 - (\theta^{(1)})^2 + 2\hat{\theta}^{(1)} - 2\theta^{(1)})x_0^{(1)} \\
& +(2\hat{\theta}^{(1)} - 2\theta^{(1)} - \hat{\theta}^{(1)}\hat{\theta}^{(2)} + \theta^{(1)}\theta^{(2)} \\
& +\theta^{(2)} - \hat{\theta}^{(2)})x_0^{(1)}x_0^{(2)} \\
& +(\hat{\theta}^{(2)} - \theta^{(2)})x_0^{(1)}(x_0^{(2)})^2 \\
& -(\hat{\theta}^{(1)} - \theta^{(1)})(x_0^{(1)})^3 m_0 \\
& -(\hat{\theta}^{(1)} - \theta^{(1)})m_0 \\
& -(\hat{\theta}^{(2)} - \theta^{(2)})x_0^{(2)} m_0 = 0
\end{aligned} \tag{20}$$

(18) is trivial and always fulfilled. Assuming that $x_0^{(1)} \neq 0$ and $x_0^{(2)} \neq 0$ respectively, (19) leads to $\hat{\theta}^{(1)} = \theta^{(1)}$ and then, (20) leads to $\hat{\theta}^{(2)} = \theta^{(2)}$. As a result, Theorem 1 is fulfilled for $T = 2$. Consequently, the parameters $\theta^{(1)}$ and $\theta^{(2)}$ are structurally identifiable.
Note that $x_0^{(1)} = 0$ and $x_0^{(2)} = 0$ is a zero measure ($x_0^{(1)} = 0$ and $x_0^{(2)} = 0$ do not belong to $\mathscr{X}_0$) that leads to a singularity and no conclusion about parametric identifiability is possible.
Besides, to retrieve the parameters from system (17), the initial condition x_0 is needed. The input/output relation approach, independent of the initial condition, is applied in the following.

3.2.2 Input/Output Relation Approach

For obtaining the input/output relation, that is $\mathscr{L}_1 = 0$, the system (16) is first iterated up to its observability index that is also its dimension ($s = n = 2$):

$$\begin{cases}
x_{k+1}^{(1)} - (1+\theta^{(1)})x_k^{(1)} - x_k^{(1)}x_k^{(2)} - m_k = 0 \\
x_{k+2}^{(1)} - (1+\theta^{(1)})x_{k+1}^{(1)} - x_{k+1}^{(1)}x_{k+1}^{(2)} - m_{k+1} = 0 \\
x_{k+1}^{(2)} - (1-\theta^{(2)})x_k^{(2)} + (x_k^{(1)})^2 m_k = 0 \\
x_{k+2}^{(2)} - (1-\theta^{(2)})x_{k+1}^{(2)} + (x_{k+1}^{(1)})^2 m_{k+1} = 0 \\
y_k - x_k^{(1)} = 0 \\
y_{k+1} - x_{k+1}^{(1)} = 0 \\
y_{k+2} - x_{k+2}^{(1)} = 0
\end{cases} \tag{21}$$

The state $x_k^{(2)}$ is not directly transmitted through y_k. Hence, $x_k^{(2)}$ is chosen to be the greatest in the following lexicographic ranking:

$$x_k^{(1)} < x_{k+1}^{(1)} < x_{k+2}^{(1)} < x_k^{(2)} < x_{k+1}^{(2)} < x_{k+2}^{(2)} \tag{22}$$

Gröbner bases approach
The software Maxima computes, with the function `poly_buchberger`, the Gröbner basis of the ideal associated to (21), with the lexicographic order (22). One of the Gröbner basis expressions is the input/output relation $\mathscr{L}_1 = 0$:

$$\begin{aligned}
&\theta^{(1)}\theta^{(2)}y_k y_{k+1} + \theta^{(2)}(-y_{k+1}^2 + y_k y_{k+1} + m_k y_{k+1}) \\
&-y_{k+2}y_k + y_{k+1}^2 - y_k^3 y_{k+1} m_k - m_k y_{k+1} + m_{k+1}y_k = 0
\end{aligned} \tag{23}$$

The other expressions of the basis are useless for our purpose since they involve the state vector. Then, the in-

put/output relation (23) is iterated and yields $\mathscr{L}_2 = 0$:

$$\begin{array}{l}\theta^{(1)}\theta^{(2)}y_{k+1}y_{k+2} + \theta^{(2)}(-y_{k+2}^2 + y_{k+1}y_{k+2} + m_{k+1}y_{k+2}) \\ -y_{k+3}y_{k+1} + y_{k+2}^2 - y_{k+1}^3 y_{k+2}m_{k+1} - m_{k+1}y_{k+2} \\ +m_{k+2}y_{k+1} = 0\end{array} \tag{24}$$

(23) and (24) can be rewritten in the form (4) for every parameter. Indeed, the function `solve` of Maxima computes successfully:

$$\begin{array}{l}\theta^{(1)} = \dfrac{Q_1(y_k,\ldots,y_{k+3},m_k,\ldots,m_{k+2})}{P_1(y_k,\ldots,y_{k+3},m_k,\ldots,m_{k+2})} \\ \theta^{(2)} = \dfrac{Q_2(y_k,\ldots,y_{k+3},m_k,\ldots,m_{k+2})}{P_2(y_k,\ldots,y_{k+3},m_k,\ldots,m_{k+2})}\end{array} \tag{25}$$

with:

$$\begin{array}{l}P_1(y_k,\ldots,y_{k+3},m_k,\ldots,m_{k+2}) = \\ y_k y_{k+1}^2 y_{k+3} - 2y_k y_{k+1} y_{k+2}^2 + (m_{k+1}y_k y_{k+1}^4 + y_{k+1}^3 \\ -(m_k y_k^3 + m_k)y_{k+1}^2 + (2m_{k+1} - m_{k+2})y_k y_{k+1})y_{k+2}\end{array}$$

$$\begin{array}{l}Q_1(y_k,\ldots,y_{k+3},m_k,\ldots,m_{k+2}) = \\ (y_{k+1}^3 - (y_k + m_k)y_{k+1}^2)y_{k+3} - y_k y_{k+2}^3 \\ +((2y_k - m_k y_k^3)y_{k+1} + 2m_{k+1}y_k)y_{k+2}^2 \\ +(m_{k+1}y_{k+1}^5 - (m_{k+1}y_k + m_k m_{k+1})y_{k+1}^4 - y_{k+1}^3 \\ +(m_k y_k^3 - m_{k+2} + m_k)y_{k+1}^2 + (m_k m_{k+1}y_k^3 \\ +(m_{k+2} - 2m_{k+1})y_k + m_k m_{k+2})y_{k+1} - m_{k+1}^2 y_k)y_{k+2}\end{array}$$

$$\begin{array}{l}P_2(y_k,\ldots,y_{k+3},m_k,\ldots,m_{k+2}) = \\ y_k y_{k+2}^2 + (-y_{k+1}^2 + m_k y_{k+1} - m_{k+1}y_k)y_{k+2}\end{array}$$

$$\begin{array}{l}Q_2(y_k,\ldots,y_{k+3},m_k,\ldots,m_{k+2}) = \\ -(y_k y_{k+1} y_{k+3} - 2y_k y_{k+2}^2 + (m_{k+1}y_k y_{k+1}^3 + y_{k+1}^2 \\ -(m_k y_k^3 + m_k)y_{k+1} + (2m_{k+1} - m_{k+2})y_k)y_{k+2})\end{array} \tag{26}$$

Thus, Theorem 2 is fulfilled and $\theta^{(1)}$ and $\theta^{(2)}$ are structurally identifiable.

Characteristic set approach

The set of polynomials defining system (16) are:

$$\begin{array}{lcl}B_1 &=& x_{k+1}^{(1)} - (1+\theta^{(1)})x_k^{(1)} - x_k^{(1)}x_k^{(2)} - m_k \\ B_2 &=& x_{k+1}^{(2)} - (1-\theta^{(2)})x_k^{(2)} - (x_k^{(1)})^2 m_k \\ B_3 &=& y_k - x_k^{(1)}\end{array} \tag{27}$$

According to the lexicographic order (22), the leader of B_1 is $x_k^{(2)}$, the leader of B_2 is $x_{k+1}^{(2)}$ and the leader of B_3 is $x_k^{(1)}$. To compute the characteristic set, polynomials B_1 and B_2 must be reduced with respect to polynomial B_3. It gives:

$$\begin{array}{lcl}B_1 &=& y_{k+1} - (1+\theta^{(1)})y_k - y_k x_k^{(2)} - m_k \\ B_2 &=& x_{k+1}^{(2)} - (1-\theta^{(2)})x_k^{(2)} - y_k^2 m_k \\ B_3 &=& y_k - x_k^{(1)}\end{array} \tag{28}$$

The leader of B_1 is $x_k^{(2)}$ and the state $x_k^{(1)}$ or its iterates does no longer appear in B_1. Consequently, B_1 is reduced with respect to B_3. The leader of B_2 is still $x_{k+1}^{(2)}$. As the state $x_k^{(1)}$ and its iterates do not appear in B_2, B_2 is reduced with respect to B_3. However, polynomial B_2 must be reduced with respect to B_1. It leads to:

$$\begin{array}{lcl}B_1 &=& y_{k+1} - (1+\theta^{(1)})y_k - y_k x_k^{(2)} - m_k \\ B_2 &=& \theta^{(1)}\theta^{(2)}y_k y_{k+1} + \theta^{(2)}(-y_{k+1}^2 + y_k y_{k+1} + m_k y_{k+1}) \\ && -y_{k+2}y_k + y_{k+1}^2 - y_k^3 y_{k+1}m_k - m_k y_{k+1} + m_{k+1}y_k \\ B_3 &=& y_k - x_k^{(1)}\end{array} \tag{29}$$

The leader of B_2 is now y_{k+2}. It is reduced with respect to B_1. The polynomials B_1, B_2 and B_3 are all autoreduced and the characteristic set is given by:

$$\begin{array}{l}A_1(y_k,y_{k+1},y_{k+2},m_k,m_{k+1},m_{k+2},\theta^{(1)},\theta^{(2)}) = B_2 \\ = \theta^{(1)}\theta^{(2)}y_k y_{k+1} + \theta^{(2)}(-y_{k+1}^2 + y_k y_{k+1} + m_k y_{k+1}) \\ -y_{k+2}y_k + y_{k+1}^2 - y_k^3 y_{k+1}m_k - m_k y_{k+1} + m_{k+1}y_k\end{array}$$

$$\begin{array}{l}A_2(y_k,y_{k+1},y_{k+2},m_k,m_{k+1},m_{k+2},\theta^{(1)},\theta^{(2)},x_k^{(1)}) = B_3 \\ = y_k - x_k^{(1)}\end{array}$$

$$\begin{array}{l}A_3(y_k,y_{k+1},y_{k+2},m_k,m_{k+1},m_{k+2},\theta^{(1)},\theta^{(2)},x_k^{(1)},x_k^{(2)}) = B_1 \\ = y_{k+1} - (1+\theta^{(1)})y_k - y_k x_k^{(2)}\end{array} \tag{30}$$

In the characteristic set (30), $A_1 = 0$ represents the input/output relation and is identical to (23) given by the Gröbner basis approach. Hence, Theorem 2 is fulfilled and the parameters $\theta^{(1)}$ and $\theta^{(2)}$ are structurally identifiable.

In the context of brute force attack, since the parameters $\theta^{(1)}$ and $\theta^{(2)}$ are identifiable, they could play the role of the secret key.
However, it is clear that, performing a known plaintext attack, the parameters $\theta^{(1)}$ and $\theta^{(2)}$ can be easily reconstructed. Hence, this cryptosystem is weak against known plaintext algebraic attack.

4 Conclusion

In this paper, a general framework based on identifiability for the cryptanalysis of a large class of chaotic cryptosystems is proposed. More precisely, it is provided a systematic methodology to test, a priori, during the design stage, whether the parameters of a chaotic cryptosystem may play the role of the secret key or not. From a cryptanalysis point of view, this paper leads to the following conclusions.

Firstly, if the parameter vector of the transmitter is identifiable, it is more difficult for the eavesdropper to find it by a brute force attack (exhaustive search). Consequently, this parameter vector may be a good candidate to play the role of the secret key against a brute force attack.
If the parameter vector is not identifiable, the eavesdropper has a higher favorable chance to find it by a brute force attack. Thus, this parameter vector is a bad candidate to play the role of the secret key against a brute force attack.

Secondly, if the parameters are identifiable, which is a necessary condition for the security against brute force attack, an explicit form of each parameter can be established. For cryptosystems involving polynomial nonlinearities, the parameters can be easily retrieved by a known plaintext attack.

As a consequence, all these cryptosystems are weak against algebraic attacks. Let us point out that this weakness is independent of the motion exhibited by the system, chaotic or not. All these results can be easily extended to the case of continuous-time chaotic systems and can be transposed to the other usual methods for hiding an information, additive masking, chaotic switching and parameter modulation.

References

[1] T. L. Carroll and L. M. Pecora. Synchronizing chaotic circuits. *IEEE Trans. Circuits and Systems*, 38(4):453–456, April 1991.

[2] M. J. Ogorzalek. Taming chaos - part I: synchronization. *IEEE Trans. Circuits. Syst. I: Fundamental Theo. Appl*, 40(10):693–699, 1993.

[3] M. Hasler. Synchronization of chaotic systems and transmission of information. *International Journal of Bifurcation and Chaos*, 8(4), April 1998.

[4] T. Yang. A survey of chaotic secure communication systems. *Int. J. of Computational Cognition*, 2(2):81–130, 2004. (available at `http://www.YangSky.com/yangijcc.htm`).

[5] G. Millérioux, A. Hernandez, and J.M Amigó. Conventional cryptography and message-embedding. In *Proc. of the 2005 International Symposium on Nonlinear Theory and its Applications (NOLTA 2005)*, Bruges, Belgium, 18-21 October 2005.

[6] H. Delfs and H. Knebl. *Introduction to cryptography*. Springer-Verlag, Berlin, 2002.

[7] X. Wang, M. Zhan, and C. H. Lai. Error function attack of chaos synchronization based encryption schemes. *Chaos*, 14(1):128–137, 2004.

[8] S. Li, G. Alvarez, G. Chen, and X. Mou. Breaking a chaos-noise-based secure communication scheme. *Chaos*, 15(1), 2005.

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

[10] G. Alvarez, S. Li, F. Montoya, G. Pastor, and M. Romera. Breaking projective chaos synchronization secure communication using filtering and generalized synchronization. *Chaos, Solitons and Fractals*, 24:775–783, 2005.

[11] R. Marino and P. Tomei. Global adaptive observers for nonlinear systems via filtered transformations. *IEEE Trans. on Automatic Control*, 37(8):1239–1245, 1992.

[12] A. Fradkov, H. Nijmeijer, and A. Markov. Adaptive observer-based synchronization for communication. *Int. J. of Bifurcation and Chaos*, 10(12):2807–2813, 2000.

[13] Q. Zhang and A. Xu. Global adaptive observer for a class of nonlinear systems. In *Proc. of the 40th IEEE Conf. on Decision and Control*, volume 4, pages 3360–3365, Orlando, Florida, 4-7 dec. 2001.

[14] A. Guyader and Q. Zhang. Adaptive observer for discrete time linear time varying systems. In *Proc. of 3th IFAC/IFORS Symposium on Identification and System Parameter Estimation, SYSID'2003*, Rotterdam, The Netherlands, August 2003.

[15] F. Anstett, G. Millerioux, and G. Bloch. Global adaptive synchronization based upon polytopic observers. In *Proc. of IEEE International symposium on circuit and systems, ISCAS'04*, volume 4, pages IV–728 – 731, Vancouver, Canada, May 2004.

[16] G. Millerioux, F. Anstett, and G. Bloch. Considering the attractor structure of chaotic maps for observer-based synchronization problems. *Mathematics and Computers in Simulation*, 68(1):67–85, 2005.

[17] H. Guojie, F. Zhengjin, and M. Ruiling. Chosen ciphertext attack on chaos communication based on chaotic synchronization. *IEEE Trans. on Circuits and Syst. - I: Fundamental Theory and Applications*, 50(2):275–279, 2003.

[18] H. Guojie, F. Zhengjin, and W. Lin. Analysis of a type digital chaotic cryptosystem. In *Proc. of the IEEE International Symposium on Circuits and Systems ISCAS*, volume 3, pages III–473–III–475, Scottsdale, Arizona, 26-29 may 2002.

[19] P. G. Vaidya and S. Angadi. Decoding chaotic cryptography without access to the superkey. *Chaos, Solitons and Fractals*, 17:379–386, 2003.

[20] E. Solak. On the security of a class of discrete-time chaotic cryptosystems. *Physics Letters A*, (320):389–395, 2004.

[21] E. Solak. Cryptanalysis of observer based discrete-time chaotic encryption schemes. *International Journal of Bifurcation and Chaos*, 15(2):653–658, 2005.

[22] T. Beth, D. E. Lazic, and A. Mathias. *Cryptanalysis of cryptosystems based on remote chaos replication*. Springer-Verlag, 1994. Advances in Cryptology-CRYPTO'94.

[23] H. Dedieu and M. Ogorzalek. Identifiability and identification of chaotic systems based on adaptative synchronization. *IEEE Trans. Circuits Syst. I: Fund. Theo. Appl*, 44(10):948–962, October 1997.

[24] F. Anstett, G. Millerioux, and G. Bloch. Message-embedded cryptosystems: cryptanalysis and identifiability. In *Proc. of the 44th IEEE Conference on Decision and Control*, pages 2548–2553, Sevilla, Spain, December 12-15 2005.

[25] M. Hénon. A two-dimensional mapping with a strange attractor. *Communications of Mathematical Physics*, 50:69–77, 1976.

[26] R.M. May. Simple mathematical models with complicated dynamics. *Nature*, 261:459–470, 1976.

[27] B. Mandelbrot. *Les objets fractals : forme, hasard et dimension*. Flammarion, Paris, 1975.

[28] H. G. Schuster. *Deterministic Chaos*. VCH Pub., New York, 1988.

[29] G. Millerioux and J. Daafouz. Unknown input observers for message-embedded chaos synchronization of discrete-time systems. *Int. J. of Bifurcation and Chaos*, 14(4):1357–1368, April 2004.

[30] G. Millerioux and J. Daafouz. Input independent chaos synchronization of switched systems. *IEEE Trans. on Automatic Control*, pages 1182 – 1187, July 2004.

[31] A. Menezes, P. Van Oorschot, and S. Vanstone. *Handbook of Applied Cryptography*. CRC Press, October 1996.

[32] E. Walter and L. Pronzato. *Identification of parametric models from experimental data*. Springer-Verlag, 1997.

[33] S. Nõmm and C. H. Moog. Identifiability of discrete-time nonlinear systems. In *Proc. of the 6th IFAC Symposium on Nonlinear Control Systems, NOLCOS*, pages 477–489, Stuttgart, Germany, September 1-3 2004.

[34] L. Ljung and T. Glad. On global identifiability for arbitrary model parametrizations. *Automatica*, 30(2):265–276, 1994.

[35] S. Diop and M. Fliess. Nonlinear observability, identifiability and persistent trajectories. In *30th Conference on Decision and Control*, pages 714–718, Brighton, England, December 1991.

[36] H. Pohjanpalo. System identifiability based on the power series expansion of the solution. *Math. Biosci.*, 41:21–33, 1978.

[37] H. Nijmeijer and A. J. van der Schaft. *Nonlinear Dynamical Control Systems*. Springer, 1990.

[38] B. Buchberger. *An algorithm for finding a basis for the residue class ring of zero-dimensional polynomial ideal*. PhD thesis, Math. Inst. Univ. of Innsbrück, Austria, 1965.

[39] E. Kolchin. *Differential algebra and algebraic groups*. 1973.

[40] Erik Frisk. *Residual Generation for Fault Diagnosis*. PhD thesis, Linköpings Universitet, Sweden, November 2001.

[41] J. F. Ritt. *Differential algebra*. Providence, RI: American Mathematical Society, 1950.

[42] J-P. Barbot. Observability bifurcations: application to cryptography. *4ème Ecole Internationale d'Automatique de Lille*, pages 1–19, 2003.