A new parameter determination method for some double-scroll chaotic systems and its applications to chaotic cryptanalysis

A.B. Orue[a], G. Alvarez[*,b], G. Pastor[b], M. Romera[b], F. Montoya[b], Shujun Li[c]

[a] *Área de Cultura Científica, CSIC, Serrano 144, 28006–Madrid, Spain*
[b] *Instituto de Física Aplicada, CSIC, Serrano 144, 28006–Madrid, Spain*
[c] *Fachbereich Informatik und Informationswissenschaft, Universität Konstanz Fach M697, Universitätsstraße 10, 78457 Konstanz, Germany*

Abstract

This paper describes a method about how to determine parameters of some double-scroll chaotic systems, including the Lorenz system and the Chua's circuit, from one of its variables. The geometric properties of the system are exploited firstly to reduce the parameter search space. Then, a synchronization-based approach, with the help of the same geometric properties as coincidence criteria, is implemented to determine the parameter values with the wanted accuracy. The method is not affected by a moderate amount of noise in the waveform. As an example of its effectiveness, the method is applied to cryptanalyze two two-channel chaotic cryptosystems, figuring out how the secret keys can be directly derived from the driving signal $z(t)$.

1. Introduction

The feasibility of synchronizing two chaotic systems [1] makes it possible to use the signals generated by chaotic systems as carriers for analog and digital communications, which soon aroused great interest as a potential means for secure communications [2]. In the literature, it is assumed that chaotic systems are adequate means for secure transmission, because they present some properties similar to pseudorandom noises used for masking signals for cryptographic purposes. These properties include sensitive dependence on parameters and initial conditions, ergodicity, mixing, and dense periodic points [3].

For over a decade a number of secure communication systems have been proposed. In a common scheme called chaotic masking, the plaintext message signal $m(t)$ is concealed into the chaotic signal by simply adding it to a system variable $u(t)$ of the sender chaotic generator [4–6], and the receiver has to synchronize with the sender to regenerate the chaotic signal $\tilde{u}(t)$ and thus to recover the message $m(t)$. This uncomplicated chaotic masking scheme can be easily broken by setting apart $u(t)$ and $m(t)$ signals using elemental high-pass filtering [7–9], or by directly estimating the chaotic signal $u(t)$ via some specific methods such as Short's NLD method [10, 11].

In order to avoid the weakness of the common chaotic masking scheme, a more elaborated mixing procedure was proposed by Jiang in 2002 [12] and later adopted by some other researchers [13, 14]. They proposed to use two transmission channels instead of only one, where the first channel transmits an unmodified chaotic system variable, and the second channel conveys a signal that was a more complicated

*Corresponding author: Email: gonzalo@iec.csic.es

non-linear combination of the plaintext and one or more system variables, from which it is impossible to retrieve any of the components. The first channel transmits the synchronizing signal to the receiver, so that the remaining chaotic system variables can be generated and employed to retrieve the plaintext from the signal received from the second channel. As long as the parameters used at the receiver are the same as those at the sender side, the plaintext can be recovered asymptomatic.

When cryptanalyzing a cryptosystem, the general assumption made is that the cryptanalyst knows exactly the design and working of the cryptosystem under study, i.e., he knows everything about the cryptosystem except the secret key. In other words, the security of a cryptosystem should depend only on its key. This is an evident requirement of today's secure communications systems, usually referred to as Kerckhoffs' principle [15, 16]. Therefore, in our attack, total knowledge of the communications system design is assumed. In the cryptosystems proposed in [13, 14], the security relies on the secrecy of the system parameters, which play the role of secret key, hence the determination of the system parameters from the chaotic ciphertext is equivalent to breaking the system.

The contribution of this work is double. First, a novel determination method of the unknown parameters of the Lorenz system, when the waveform of one of its variables is known, is presented in Sec. 2. Then, in Secs. 3 and 4, it is shown how this method can be applied to break two different two-channel cryptosystems that use the Lorenz system [13, 14]. Finally, Sec. 7 concludes the paper.

2. Parameter determination of the Lorenz system

Since 1963 the Lorenz system [17] has been a paradigm for chaos. Consequently, it has been predominantly used in the design of chaotic cryptosystems. It is defined by the following equations:

$$\begin{aligned} \dot{x} &= \sigma(y - x), \\ \dot{y} &= rx - y - xz, \\ \dot{z} &= xy - bz. \end{aligned} \tag{1}$$

where σ, r and b are fixed parameters.

The proposed approach to the problem of Lorenz system parameter determination is based on a homogeneous driving synchronization mechanism [18] between a drive Lorenz system and a response subsystem that is a partial duplicate of the drive system reduced to only two variables, driven by the third variable.

Projective synchronization (PS) is an interesting phenomena firstly described by Mainieri and Rehacek [19]. It consists of the synchronization of two partially linear coupled chaotic systems, a sender (master/drive) system and a receiver (slave/response) system, in which the amplitude of the slave system is a scalar multiple, called scaling factor, of that of the sender system in the phase space. The original study was restricted to three-dimensional partially linear systems. Xu and Li [20] showed that PS could be extended to general classes of chaotic systems without partial linearity, by means of the feedback control of the slave system.

The response system is defined by the following equations, in which variable $z(t)$ is used as the driving signal:

$$\begin{aligned} \dot{x}_r &= \sigma^*(y_r - x_r), \\ \dot{y}_r &= r^* x_r - y_r - x_r z, \end{aligned} \tag{2}$$

where σ^* and r^* are fixed parameters.

As was shown in [18, §III] this drive-response configuration has two conditional Lyapunov exponents, the first one is fairly negative while the second one is of small positive value, thus leading to a slightly unstable system. The consequence is that if the parameters of drive and response systems are identical, then the drive and response variables will become identical (for complete synchronization) or differ only in an scaling factor (for projective synchronization), that depends on the initial conditions of the drive and response systems. However, if the parameters are not exactly equal, then the drive and response variables will be completely different.

When the drive and response systems parameters are equal, the variable $x_r(t)$ will be easily recognizable as the familiar waveform of a Lorenz system, by a supposed human skilled observer. But if drive and response systems parameters are different, the waveforms generated by the response system will be a nonsense mesh some seconds after the beginning of driving, due to the sensitive dependence of chaotic systems on parameter values. This phenomenon could be interpreted by the observer as the consequence of a wrong parameter guessing.

This work describes a criterion, based on the study of some geometric properties of the waveforms of Lorenz system's variables, to automatically decide if the response system parameters coincide with the drive system parameters or not, by means of the analysis of the $x_r(t)$ waveform of the response system.

This method of recovering the unknown system parameters is applicable to cryptosystems that use the variable $z(t)$ as the driving signal like those chaotic cryptosystems proposed in [13, 14]. But it is not applicable to other two-channel cryptosystems driven by $x(t)$ or $y(t)$, like [12], because in those cases both conditional Lyapunov exponents are negative and the drive-response configuration is stable, in spite of being the drive and response parameters moderately different.

To minimize the computer workload as much as possible, the parameter search space is previously reduced to a narrow range by means of a simple measure upon the $z(t)$ waveform. Then, all the unknown parameter values are determined with the desired accuracy.

There exist several efficient methods of identifying parameters of chaotic systems such as the Lorenz system. Stojanovski *et al.* [21] have described a generic method to simultaneously identify all the three parameters of the Lorenz system when one of the variables $x(t)$ or $y(t)$ were known. Parlitz [22] also reported a method to recover the parameters r and b of the Lorenz system when $y(t)$ is known, by means of auto-synchronization based on a Lyapunov function. Recently, Huang [23], Yu and Parlitz [24] have extended the above method to general systems, showing that all the system parameters can be retrieved when all the state variables are measurable. They illustrated the procedure by applying it to the parameter identification problem of the Lorenz system. Yu and Liu [25] have introduced an adaptive synchronization approach that allows the determination of all parameters of the Lorenz system when only the state variable $x(t)$ is known. Orue *et al.* [26] reported that a geometric method can determine the parameters σ and r, when the state variable $x(t)$ is known. An application to cryptanalysis of two-channel chaotic cryptosystems is also reported in [26]. Alvarez *et al.* [27] proposed a generalized synchronization based method to determine the parameters σ and r when the combination of state variables $x(t) + y(t)$ is known, which was used for cryptanalysis of a projective synchronization chaotic cryptosystem. Parlitz *et al.* [28] described a general parameter estimation method that recovers the parameter values of a given model from a single time series, by minimizing an averaged synchronization error, which was demonstrated with the Hénon map and Chua's circuit.

Note that all those parameter determination methods take advantage of the fact that all the conditional Lyapunov exponents of the response system are negative. In contrast, the identification procedure described in this paper works for response systems with one positive conditional Lyapunov exponent, which in the case of the Lorenz system corresponds to the use of the variable $z(t)$ as the driving signal.

2.1. Lorenz attractor's geometric properties

According to [17], the Lorenz system has three fixed points. For $0 < r < 1$, the origin of coordinates is a globally stable fixed point; for $1 \leq r < r_c$, the origin becomes unstable, giving rise to two other stable twin points C^+ and C^-, of coordinates $C^{\pm} = (\pm\sqrt{b(r-1)}, \pm\sqrt{b(r-1)}, (r-1))$, being r_c a critical value defined as:

$$r_c = \frac{\sigma(\sigma + b + 3)}{\sigma - b - 1}. \tag{3}$$

When r exceeds the critical value r_c, the system becomes unstable, and its behavior is chaotic.

Figure 1(a) shows the well-known double-scroll Lorenz attractor formed by the projection on the x-z plane, in the phase space, of a trajectory portion extending along 10 seconds, where the parameters are $r = 45.6$, $\sigma = 16$, $b = 4$, the initial conditions are $x_0 = 13.3566$, $y_0 = 13$, $z_0 = 44.6$, and the asterisks denote the fixed points C^+ and C^-.

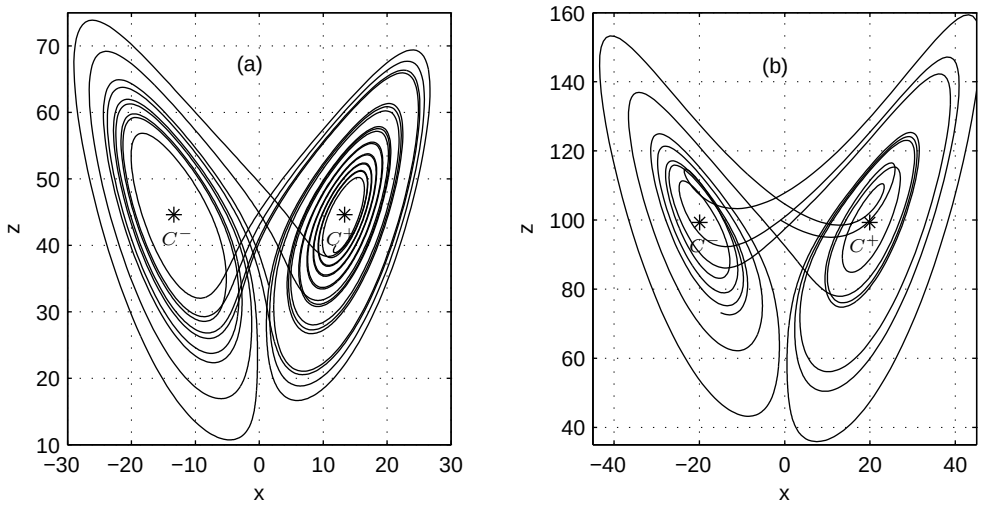

Figure 1: Lorenz chaotic attractor: (a) parameters $r = 45.6$, $\sigma = 16$ and $b = 4$; (b) parameters $r = 100.3$, $\sigma = 16$ and $b = 4$, showing irregular cycles that not surround the fixed points. The positions of the fixed points C^+ and C^- are indicated by asterisks.

It is well-known that the Lorenz attractor's trajectory follows two loops, in the vicinity of the fixed points C^+ and C^-, with a spiral-like shape of steadily growing amplitude, jumping from one to the other, at irregular intervals, in a random-like manner though actually deterministic [17]. Whenever the jump happens, the trajectory almost jumps from one loop of a high amplitude to another loop of smaller amplitude. The spiraling trajectory may pass arbitrarily near to the fixed points, but never reach them while in chaotic regime.

Definition 1. The portions of the attractor's trajectory that consists of a revolution of 360° beginning after a change of sign of x and y are *irregular cycles*. The portions of the trajectory that constitute a complete spiral revolution of 360° and do not begin after a change of sign of x and y are *regular cycles*.

Remark 1. Regular cycles always surround the fixed points C^+ or C^-, taking them as centers of a growing spiral.

Remark 2. Irregular cycles usually surround the fixed points C^+ or C^-; but sometimes may not surround them, instead the trajectory may pass slightly above them in the x-z plane. This phenomenon is illustrated in Fig. 1(b), with system parameters $r = 100.3$, $\sigma = 16$, $b = 4$, and initial conditions $x_0 = -1$, $y_0 = 35.24$, $z_0 = 100$.

Definition 2. The *attractor eyes* are constituted by the two neighborhood regions around the fixed points that are not filled with regular cycles. The eye centres are the fixed points C^+ or C^-.

Definition 3. The *eye aperture* x_a and z_a of the variables x and z, for a particular time period, is the smallest distance between the maxima and minima of $|x(t)|$ and $z(t)$, respectively, of the regular cycles, measured along this time period.

Figure 2 illustrates the first 2.25 seconds of another version of the Lorenz attractor of Fig. 1(b), folded around the z axis and formed by the projection on the x-z plane, in the phase space, of a trajectory portion of $z(t)$ and $|x(t)|$. The trajectory portion drawn with solid thick line is the regular cycle closest to the fixed points $C^{\pm}$, from which the eye aperture of x_a and z_a can be determined. The trajectory portion drawn with dashed thick line belongs to the preceding irregular cycle.

2.2. Reduction of the parameters search space

The geometric properties of Lorenz system allows for a previous reduction of the search space of the parameter r, before carrying out the accurate parameter determination, taking advantage of the relation of the system parameter r with the coordinates $z_{C^+} = z_{C^-} = r - 1$ of the fixed points C^+ and C^- and Eq. (3).

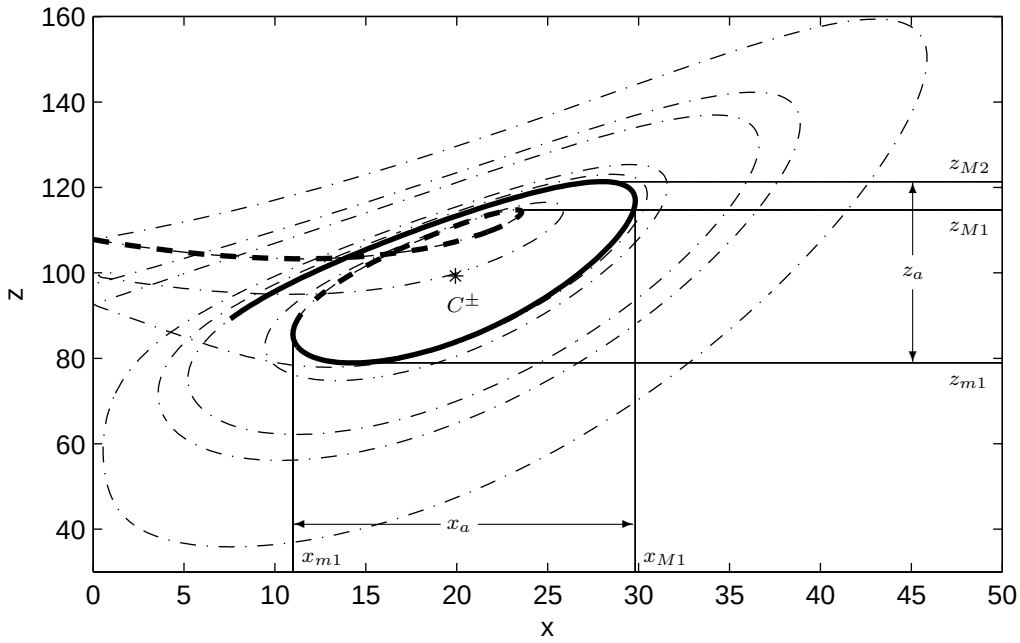

Figure 2: First 2.25 seconds of a version of the Lorenz attractor of Fig. 1(b), folded around the z axis. The solid thick line trajectory portion is the regular cycle closest to the fixed points $C^{\pm}$. The dashed thick line trajectory portion is the preceding irregular cycle.

The estimated value $z^*_{C^{\pm}}$ of the fixed points coordinates $z_{C^+} = z_{C^-}$ was calculated from the variable $z(t)$ using following algorithm:

1. compile a list of all the relative maxima and minima of $z(t)$,
2. exclude all the minima belonging to an irregular cycle from the list,
3. retain the biggest relative minimum z_{m1}, among the remaining list elements,
4. select the two maxima z_{M1}, z_{M2} immediately preceding and following z_{m1}, respectively,
5. calculate the spiral centre as $z^*_{C^{\pm}} = (\frac{1}{3} z_{M1} + \frac{2}{3}\ z_{M2} + z_{m1})/2$.

There is no need to find a rule of growing for the spiral radius, since the optimal values of the two weights of z_{M1} and z_{M2}, in the preceding $z^*_{C^{\pm}}$ formula, can be determined experimentally.

The minima of the irregular cycles were discarded because they are inappropriate for the fixed point's z coordinate calculation, since irregular cycles may not take the fixed points as centres. Those cycles are very easy to detect from the $z(t)$ waveform: they are the first minima that comes after a previous minimum of smaller value.

Figure 3 illustrates the relative error when the value of r is estimated as $r^* = z^*_{C^{\pm}} + 1$, for values of r^* ranging from the critical value $r^* = r_c$ to $r^* = 120$, in increments of $\Delta r^* = 1$, for 15 different combinations of system parameters, $\sigma = 6, 10, 13, 16, 20$ and $b = 2, 8/3, 4$. The analyzed time was 200 seconds of the $z(t)$ waveform. As can be seen, the maximum relative error spans from -0.23% to $+0.3\%$. In this way, when trying to guess the value of r from the waveform of $z(t)$, the effective search space may be reduced to a narrow margin of less than 0.6% of the computed value $r^* = z^*_{C^{\pm}} + 1$.

The presence of moderate noise added to the $z(t)$ waveform did not affect the precision of the measure. Some tests were made by adding either white gaussian noise or sinusoidal signals, of a level 30 db below $z(t)$. The resultant relative error in the guess of r^* was still inferior to $\pm 0.2\%$, for $\sigma = 16$ and $b = 4$. But for noise of larger amplitude, the increase of relative error was noticeable. For instance, when the noise reached a value of 20 dB below $z(t)$, the relative error raised to about $\pm 1\%$.

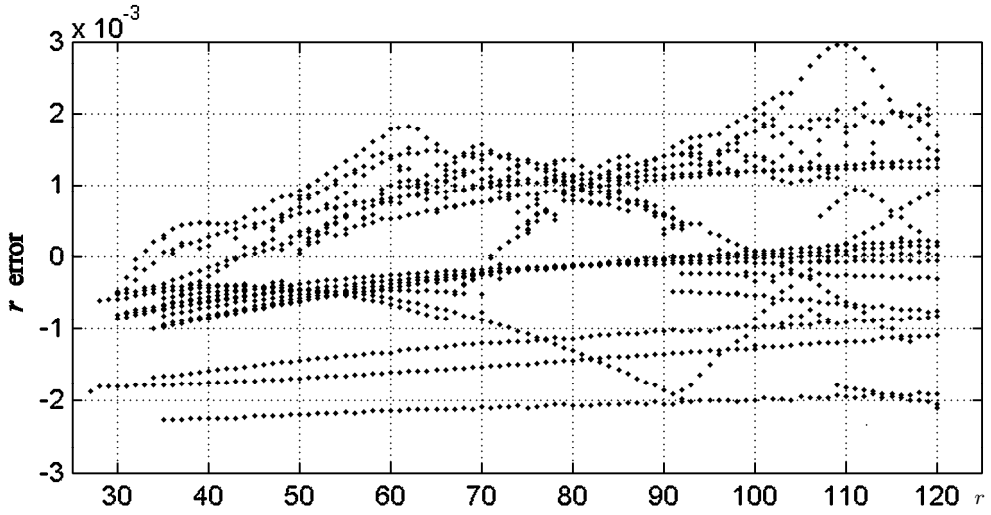

Figure 3: The estimation error of the parameter r, when calculated from the fixed-point coordinate $z^*_{C^\pm}$, for different combinations of system parameters σ and b.

The search space of σ^* can also be delimited. Assuming that $r > r_c$, $b \geq 0$ and $\sigma > 0$, it follows from Eq. (3) that:

$$0 > \sigma^2 + (b + 3 - r)\sigma + r(b + 1) > \sigma^2 + (3 - r)\sigma, \tag{4}$$

which yields a very conservative margin of $0 < \sigma < r - 3$.

2.3. Accurate parameter determination

Once the search space of the parameters is fixed, a homogeneous driving synchronization based procedure can be implemented to determine the approximate values r^* and σ^* with any desired accuracy. For this purpose, the response system described by Eq. (2) was used.

When the synchronizing signal is fed to the response and the parameters of both systems agree, i.e. $r^* = r$ and $\sigma^* = \sigma$, the variables x_r and y_r follow the drive signals x and y with a scale factor that depends on the initial conditions. If the parameters of both systems do not agree, i.e. $r^* \neq r$ and/or $\sigma^* \neq \sigma$, the variables waveforms of drive and response systems will differ absolutely, even if the initial conditions are the same. After a few system iterations, all waveforms generated with different parameter values are nearly alike, but as the number of iterations grow, the waveforms generated with different parameter values begin to diverge, due to the conditional positive Lyapunov exponent of the drive-response configuration. For large number of iterations, even the smallest difference in parameter values leads to a serious disagreement of drive and response waveforms.

Figure 4 shows the double-scroll Lorenz attractor formed by the projection on the x_r-z plane when four possible cases of parameter coincidence are considered. In Fig. 4(a), both parameters of drive and response systems are equal. It can be seen that the attractor is similar to the illustrated in Fig. 1(a), being the difference the disagreement in the horizontal scale due to different initial conditions. It can also be observed that the attractor eye is quite open. In Fig. 4(b), one parameter coincides, but the other differs: $\sigma = \sigma^* = 16$, $r = 45.6$ and $r^* = 45.61$. It can be seen that eye aperture has diminished considerably with respect to the former case. In Fig. 4(c), the coinciding parameter is $r = r^* = 45.6$, the differing one is $\sigma = 16$ and $\sigma^* = 15.65$. It can be seen that the eye aperture has diminished even more. Finally, in Fig. 4(d), both parameters differ: $r = 45.6$, $r^* = 45.61$, $\sigma = 16$ and $\sigma^* = 15.65$. It can be seen that the eye is completely closed, i.e. the eye x-aperture x_a is negative. Similar experiments were carried out for a great variety of parameter values of the driving system, and we got similar results. When the differences between the true parameter values and the guessed values (i.e., $r - r^*$ and $\sigma - \sigma^*$) are big, the eye aperture closes after very few cycles. As the differences become smaller, the number of cycles needed to obtain a closing eye goes down.

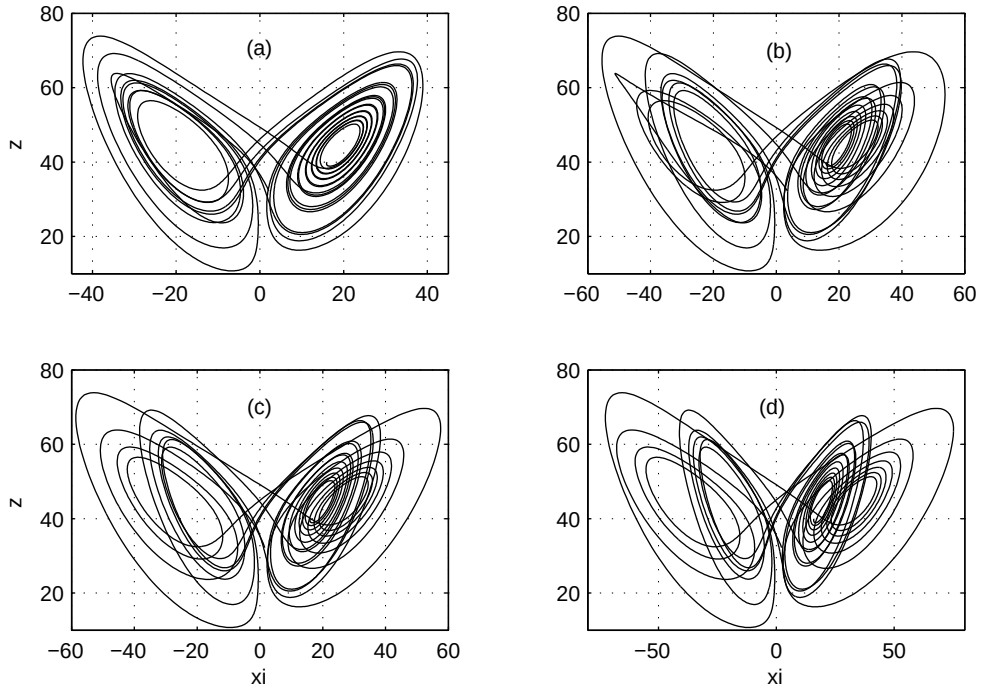

Figure 4: Lorenz attractor formed by the projection on the x_r-z plane, with the same drive parameters: $\sigma = 16$ and $r = 45.6$, but different response parameter values: (a) $\sigma^* = \sigma$, $r^* = r$; (b) $\sigma^* = \sigma$, $r^* = 45.61$; (c) $\sigma^* = 15.65$, $r^* = r$; (d) $\sigma^* = 15.65$, $r^* = 45.61$.

The value of the eye x-aperture x_a of the variable $x_r(t)$ was computed for many sets of parameters values. It was found in all cases that its maximum value was reached when $r^* = r$ and $\sigma^* = \sigma$. For these parameter values the variables x and x_r are completely synchronous but differ only in a proportionality factor. Hence the maximum eye aperture is an excellent numerical criterium for evaluating the synchronism between drive and response systems.

The eye x-aperture x_a of the variable $x_r(t)$, was calculated with the following algorithm:

1. compile a list of all relative maxima and minima of abs($x_r(t)$),
2. exclude all the maxima belonging to an irregular cycle from the list,
3. retain the smallest relative maximum x_{M_1}, among the remaining maxima,
4. select the biggest minimum x_{m1}, among all the minima,
5. calculate the eye aperture as $x_a = x_{M1} - x_{m1}$.

3. Cryptanalysis of the two-channel chaotic cryptosystem [13]

In a recent article [13], Wang and Bu proposed a new encryption scheme based on PS. Following [19], the state vector of a partially linear system of ordinary differential equations is broken in two parts $(\mathbf{u}, z)$. The equation for $z(t)$ is nonlinearly related to other variables, while the derivative of the vector $\mathbf{u}$ is linearly related to $\mathbf{u}$ through a matrix M that may depend on the variable $z(t)$. It involves a sender system $(\mathbf{u}_s, z)$, a receiver system $(\mathbf{u}_r, z)$, and an auxiliary system $(\mathbf{u}_c, z)$ defined as:

$$\begin{aligned} \dot{\mathbf{u}}_s &= M(z) \cdot \mathbf{u}_s, \quad \dot{z} = f(\mathbf{u}_s, z), \\ \dot{\mathbf{u}}_r &= M(z) \cdot \mathbf{u}_r, \\ \dot{\mathbf{u}}_c &= M(z) \cdot \mathbf{u}_c, \end{aligned} \tag{5}$$

where $\mathbf{u}_s = (x_s, y_s)$, $\mathbf{u}_r = (x_r, y_r)$, and $\mathbf{u}_c = (x_c, y_c)$. When PS takes place, we have $\lim_{t\to\infty} \|\mathbf{u}_r - \alpha \mathbf{u}_s\| = 0$, being α a constant depending on the initial conditions $\mathbf{u}_r(0)$ and $\mathbf{u}_s(0)$.

The ciphertext $s(t)$ is a time-division signal determined by $z(t)$ and $x_s(t)$ as follows:

$$s(t) = \begin{cases} x_s(t), & n\Delta t \le t \le n\Delta t + \delta t, \\ z(t), & n\Delta t + \delta t < t \le (n+1)\Delta t, \end{cases} \quad n = 0, 1, 2, \ldots, \tag{6}$$

where Δt and δt are two time intervals satisfying the following relationship: $\delta t \ll \Delta t$.

The role of the ciphertext is double: the driving signal for chaos synchronization between the sender and receiver by means of $z(t)$, and the message carrier through $x_s(t)$.

It is supposed that the plaintext message $i(t)$ was previously discretized in time, in the form of a string of bits or a string of samples, i_n. In the first case, the bits are coded as $+1$ or -1. In the second case, the analog signal is sampled at a rate of $1/\varepsilon$ Hz, where ε is the sampling period.

The encryption of a plaintext $i(t)$ is achieved as follows: at the beginning of each time interval Δt, during a much shorter time interval δt, the sender system vector $\mathbf{u}$ is forcibly modified in the following way:

$$\mathbf{u}_s(t_n) = i_n \mathbf{u}_c(t_n), \tag{7}$$

and at the end of the time interval δt the entire system is let freely evolve until the beginning of the next time period Δt.

Figure 5 illustrates the waveform of the ciphertext. It can be seen that $s(t)$ is a discontinuous signal that agrees most of the time with the function $z(t)$, but jumps to the value of $x_s(t)$ during a small time interval δt every Δt seconds.

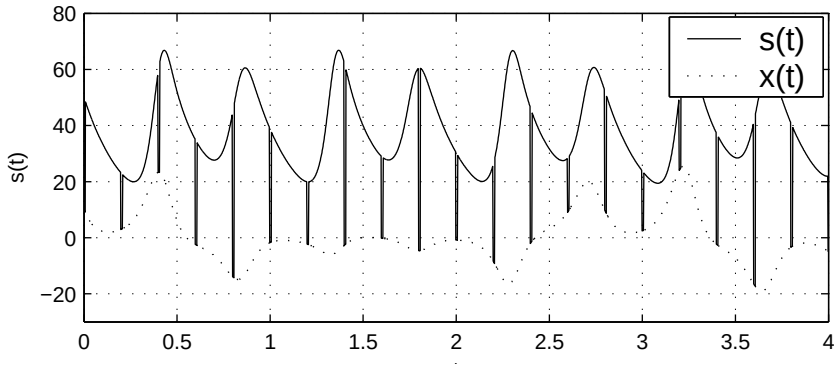

Figure 5: The scalar variable $x_s(t)$ (dotted line) and the ciphertext $s(t)$, for $\Delta t = 0.2$ and $\delta t = 0.01$ (solid line).

The function $z(t)$ can be easily recovered, at the receiver end, by filtering out the spikes. The final signal distortion is negligible due to the short spike time length δt related to their repetition period Δt.

To recover the plaintext, instead of using the signal $x_s(t)$, which is not available at the receiver end, the average value of the spike $\bar{x}_s(t)$ during the time period $n\Delta t \le t \le n\Delta t + \delta t$ is employed. Thanks again to the fact that $\delta t \ll \Delta t$, it can be considered that $\bar{x}_s(t)$ is a good approximation of $x_s(t)$.

The recovered plaintext $i'_n(t)$ at the receiver end is calculated as:

$$i'_n(t) = \frac{\bar{x}_s(t_n)}{x_r(t_n)} = \frac{\bar{y}_s(t_n)}{y_r(t_n)}. \tag{8}$$

If the initial conditions of the auxiliary system and the receiver system are identical, the original plaintext and the retrieved plaintext will agree: $i'_n(t) = i_n(t)$. However, if the initial conditions are different, the retrieved plaintext will not be equal, but proportional, to the original plaintext: $i'_n(t) = c\, i_n(t)$. Due to PS between the sender and the receiver, here c is a constant.

For practical purposes, the present system is a time-division two-channel communication system, with the particularity that two signals, one continuous and another sampled, are transmitted in a multiplexed way and later demultiplexed at the receiving end.

In [13, §3], an example was presented by using sender-receiver circuits based on the Lorenz system Eq. (1), which are similar to those described in [29]. The parameter values used are as follows:

$$\sigma = 16.0,\ r = 45.6,\ b = 4.0,\ \Delta t = 0.2,\ \delta t = 0.01,\ \varepsilon = 0.001. \tag{9}$$

It was shown that an absolute error of $\Delta r^* = 0.001$ for the parameter r^* leads to a plaintext recovery failure, and it was asserted that a similar deviation in the receiver parameter σ^* value has the same effect. Hence, although not clearly stated in [13], we can assume that in this cryptosystem the parameter values play the role of secret key. It deserves mention that designers of many chaotic cryptosystems did not clearly define the key, although they should have done so according to one of the rules described in [30].

The authors of [13] claimed that this method has some remarkable advantages over other chaos-based secure communication schemes, because it is not possible to extract the plaintext directly from the ciphertext by means of an error function attack, due to the system's high sensitivity to the parameter values. Moreover, conventional return map attacks exploiting the perturbation of the sender dynamics are also avoided, because the modulation procedure only affects the initial values of the trajectories in the phase space.

In the system proposed in [13], the variable $z(t)$ is extracted from the ciphertext $s(t)$ at the receiver end and used to achieve the synchronization with the sender. This fact allows us to mount an attack against the system parameters, whose values can be accurately determined.

In our simulation, the same sender as the one used in [13] was employed as a drive system, which is described by Eq. (1). The intruder's receiver system is described by Eq. (2). We used the same parameters employed by the authors of [13]. The initial conditions of the sender system were arbitrarily chosen as $x_s(0) = 40$, $y_s(0) = 40$, $z(0) = 40$, because in [13] there is no detail about them. The initial conditions of the intruder's response system were arbitrarily chosen as $x_r(0) = 70$, $y_r(0) = 7$.

The adequate search range for the parameters r^* and σ^* were determined as follows: applying the algorithm described in the Section 2.2 to 200 seconds of the $z(t)$ waveform, it was found that the fixed point z coordinate was $z^*_{C^\pm} = 44.5943$, which corresponds to $r^* = 45.5943$ (very close to the true value $r = 45.6$). Hence, a practical search range of r^* from $r^* = 45.50$ to $r^* = 45.70$ was selected, which is equivalent to an error allowance from -0.23% to $+0.2\%$ and compliant with Fig. 3. The search space of σ^*, according to Eq. (4), should be comprised in the range $0 < \sigma^* < 42.70$.

Figure 6 illustrates the determination process of r^* and σ^* using the procedure described in Sec. 2.3, which is accomplished in five steps. In the first step, the eye aperture of the receiver's x_r variable was measured along a period of 25 seconds, which is equivalent to 55 periods of $z(t)$. The measure was made for each of the 210 different sets of parameter values obtained by varying r^* from $r^* = 45.50$ to $r^* = 45.70$ with an incremental step $\Delta r^* = 0.05$ and varying σ^* from $\sigma^* = 1$ to $\sigma^* = 42$ with an incremental step $\Delta\sigma^* = 1$. The results are illustrated in Fig. 6(a). It can be seen that for most combinations of parameter values the aperture is negative, i.e. the corresponding parameter values are far from the right value. The best values for σ^* are comprised between $\sigma^* = 15.5$ and $\sigma^* = 16.5$, while the best values for r^* between $r^* = 45.55$ and $r^* = 45.65$. Those values are taken as the search limits in the next step. The same measure was done, in the second, third and fourth steps, during periods of 80, 250 and 800 seconds, respectively. The results are depicted in Figs. 6(b), 6(c) and 6(d).

If the available ciphertext is unlimited, the next measure step (i.e., the fifth step) could be done over a period longer than 800 seconds until the desired parameter precision is reached. But let us suppose that there is no more than 800 seconds of available ciphertext. In that case, the only choice is to constrict the search space around the last best result obtained, with a growing resolution, until it becomes impossible to decide which is the best parameter value. Figure 6(e) illustrates this situation. It was obtained by keeping the last measure period of 800 seconds, but narrowing the search space around the last best result obtained. It can be seen that the discrimination limit of the identification method was reached for that period of measure, because multiple peaks gave approximately the same eye aperture of $x_a \approx 9.2$. The four peaks of greater amplitude suggest four sets of equally plausible potential candidates of response system parameter

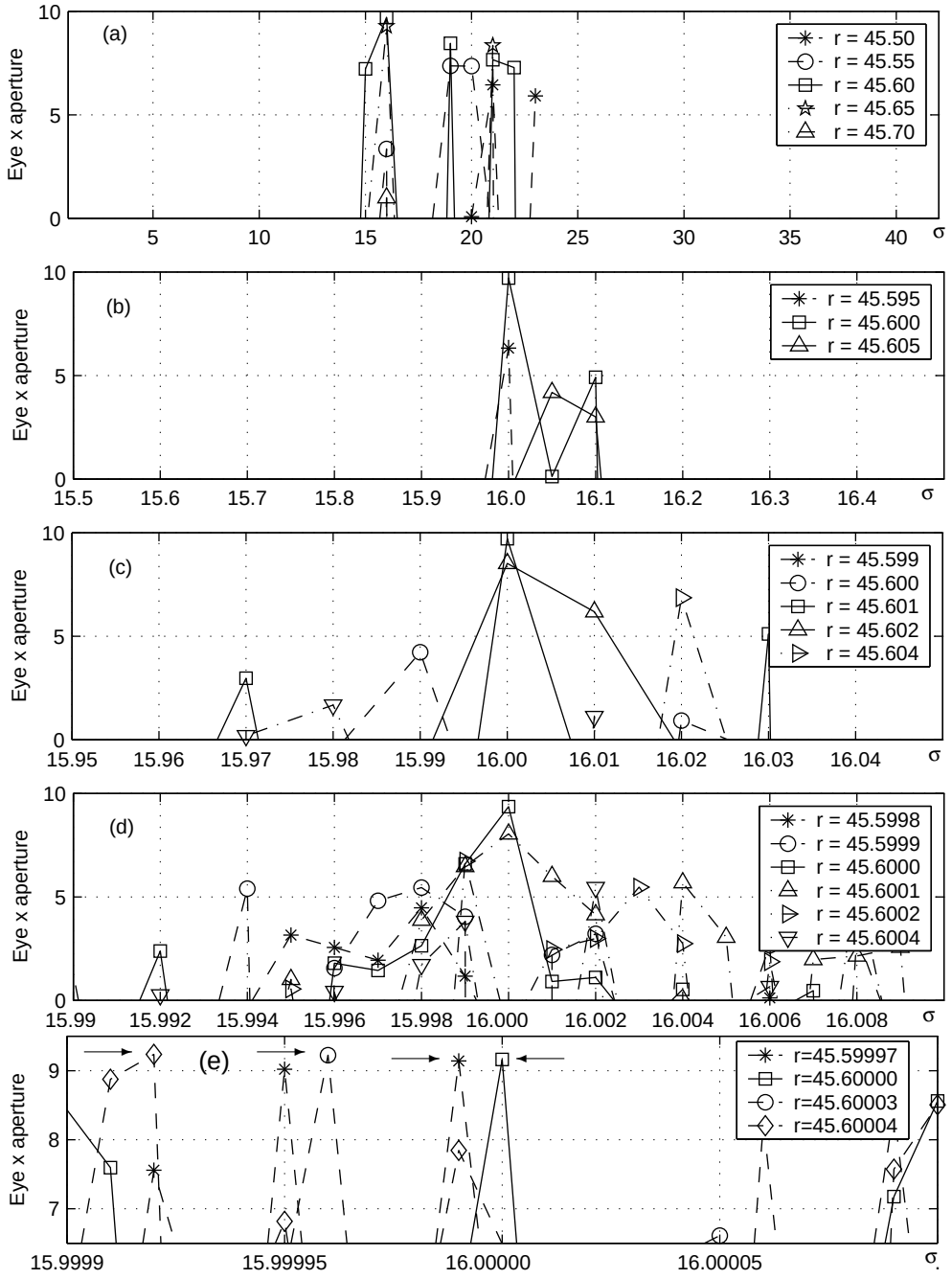

Figure 6: The eye aperture x_r of the intruder's receiver system for various measure periods: (a) 25 seconds; (b) 80 seconds; (c) 250 seconds; (d) 800 seconds; (e) 800 seconds.

sets. One of them is the right one $r_0^* = r = 45.60000$, $\sigma_0^* = \sigma = 16.00000$. The other three are slightly inexact and differ at the seventh significant digit from the right value: $r_1^* = 45.59997$, $\sigma_1^* = 15.99999$; $r_2^* = 45.60003$, $\sigma_2^* = 15.99996$ and $r_3^* = 45.60004$, $\sigma_3^* = 15.99992$.

Figures 7(a)–(c) illustrate the first 800 seconds of the waveform of $x_r(t)$ plotted against $x(t)$, for the three inexact system parameter sets. It can be seen that the $x_r(t)$ and $x(t)$ waveforms are perfectly correlated

in all the three cases despite of the inexactitude of the parameter values. Different initial conditions are the cause of the initial transitory, which lasts only 0.5 seconds and of different scale amplitudes of the waveforms. This means that any of the four potential candidates of response system parameter sets may be used indistinctly to generate the $x_r(t)$ waveform without noticeable error, for the limited time period that was considered for their determination.

For practical purposes, a limited precision in the determination process of the parameters is not a shortcoming, because the coincidence degree between two eye apertures x_{a1} and x_{a2}, corresponding to two different sets of response system parameters, is actually a measure of the coincidence degree between the two waveforms $x_{i1}(t)$ and $x_{i2}(t)$. This means that if two sets of slightly different response system parameters have the same eye apertures, computed along a limited time period, then the corresponding waveforms are practically equal during this time.

On the contrary, the parameter values shown in Fig. 7(d) correspond to an example illustrated in [13], with parameter values $r_4^* = 45.601$ and $\sigma_4^* = 15.999$, which undergo a guessing error at the fifth significant digit. In [13] such an error was considered unacceptable for correct plaintext recovery. Effectively, it can be seen in Fig. 7(d) that $x_r(t)$ and $x(t)$ waveforms are not correlated at all.

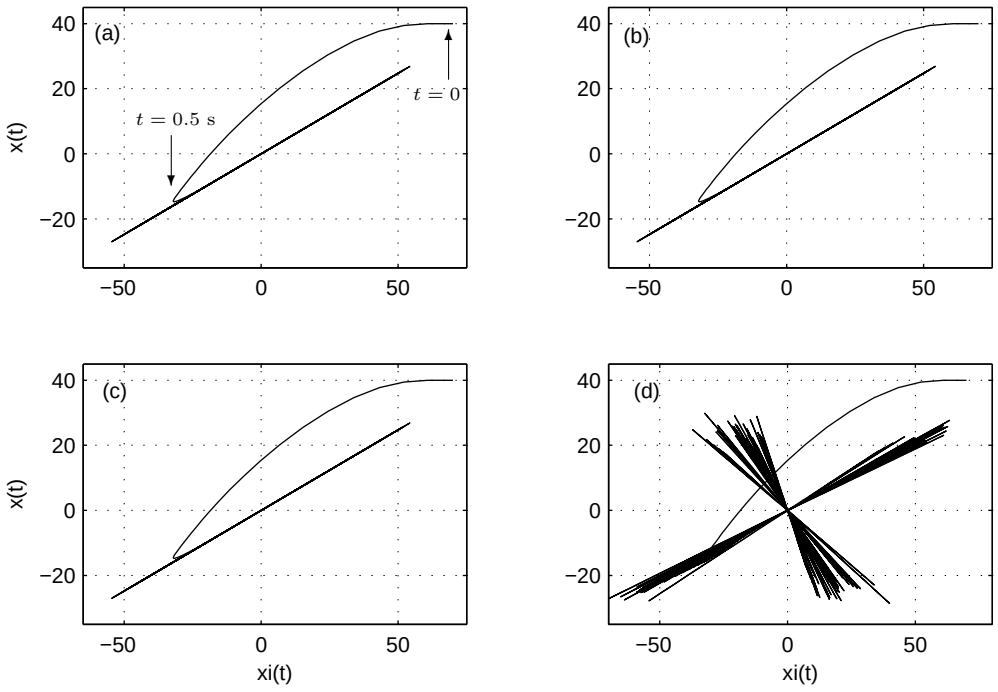

Figure 7: First 800 seconds of the phase portrait of the intruder's receiver system, for various sets of response system parameters: (a) $r^* = 45.59997$, $\sigma^* = 15.99999$; (b) $r^* = 45.60003$, $\sigma^* = 15.99996$; (c) $r^* = 45.60004$, $\sigma^* = 15.99992$; (d) $r^* = 45.601$, $\sigma^* = 15.999$.

If a greater precision of parameter determination is needed, the time period of measure could be accordingly enlarged. The maximum allowable precision is limited by the lifespan of the intercepted communication. To get an infinite precision an infinite measure period time will be needed.

When dealing with very long encrypted messages it may be unpractical to expand the parameter computation time to the whole message length, because the computation time may become too long. It then becomes better to divide the message into fractions of no more than a specific period of time such as 1000 seconds, and repeat the parameter determination procedure for each fraction. In that way, it may happen that the identified parameters will be different for each message fraction.

Once the best values of r^* and σ^* are determined, the plaintext can be retrieved in the same way as the legal key owner does.

4. Cryptanalysis of the two-channel chaotic cryptosystem [14]

After their research in PS, Xu and Li proposed a secure communication scheme based on PS chaotic masking [14], that was shown to be breakable by filtering and by generalized synchronization using the feedback of the plaintext recovery error [27]. They illustrated the feasibility of the scheme with two examples, one of which is based on the Lorenz system with sender variables $x_s(t), y_s(t)$ and $z(t)$. The transmitted signals are the shared scalar variable $z(t)$ and the ciphertext signal defined by $U(t) = x_s(t) + y_s(t) + m(t)$, where $m(t)$ is the plaintext. The retrieved plaintext is calculated by the authorized receiver as $m(t) = U(t) - (x_r(t) + y_r(t))/\alpha$, where α is the PS scaling factor and $x_r(t)$, $y_r(t)$ are the variables generated by the response system. The authors claimed that the lack of knowledge of the value of α by an intruder is an important feature to ensure the information security. In their example, the system parameter values are $\{\sigma, r, b\} = \{10, 60, 8/3\}$, the scaling factor is $\alpha = 5$, and the plaintext is a sound signal coming from a water flow, of unknown frequency spectrum and about of amplitude 0.2, approximately 0.005 times of the amplitude of $x_s(t) + y_s(t)$.

Since no detail about the initial conditions of the sender system was given in [14], we simulated this cryptosystem with arbitrarily chosen initial conditions $x_s(0) = 3$, $y_s(0) = 3$, $z(0) = 20$. The initial conditions of the intruder's response system were chosen to be $\alpha = 5$ times of the corresponding initial conditions of the sender system, i.e., $x_r(0) = 15$ and $y_r(0) = 15$. The plaintext message was chosen to be $m(t) = 0.2\sin(60\pi t)$, i.e. a low-frequency tone of similar amplitude to the example in [14].

To break this scheme, the same determination procedure described in the previous section was employed. First, using the algorithm described in Sec. 2.2, we found that the z-coordinate of the fixed point was $z^*_{C^\pm} = 58.9766$, which corresponds to $r^* = 59.9766$ (very close to the true value $r = 60$). Hence, a practical search range of r^* from $r^* = 59.8$ to $r^* = 60.2$ was selected, which is equivalent to an error allowance of $\pm 0.33\%$ and compliant with the error margins shown in Fig. 3. The search space of σ^*, according to Eq. (4), should be in the range $0 < \sigma^* < 57$.

Figure 8 illustrates the first and fifth steps of the determination procedure of the parameter r^* and σ^*, which was accomplished with the same method described in the previous section. In the first step, the eye aperture of the receiver x_r variable was measured along a period of 8 seconds, by varying r^* from $r^* = 59.8$ to $r^* = 60.2$ and σ^* from $\sigma^* = 0$ to $\sigma^* = 57$. The results are illustrated in Fig. 8(a). As in the previous section, it was supposed that the available ciphertext had a length of 800 seconds. In Fig. 8(b), it can be seen that the discrimination limit of the identification method was reached for that period of measure, giving multiple peaks with approximately the same eye aperture.

The four peaks of greater amplitude suggest four sets of potential candidates of the parameter sets of the response system. The greatest of them, with an eye aperture $x_{a0} = 37.25$, is the right one: $r^*_0 = r = 60$, $\sigma^*_0 = \sigma = 10$. The other three candidates, shown as follows in descending order of eye aperture, are slightly inexact, differing at the seventh significant digit from the right value: $r^*_1 = 59.99999$, $\sigma^*_1 = 10.00002$ ($x_{a1} = 37.23$); $r^*_2 = 60$, $\sigma^*_2 = 10.00001$ ($x_{a2} = 37.18$); and $r^*_3 = 60$, $\sigma^*_3 = 9.99998$ ($x_{a3} = 37.15$).

An approximated value of the inverse of the scaling factor α^* may be achieved by dividing, sample by sample, a time period T of the ciphertext by the corresponding period of response system sum of variables and taking the average along that time period:

$$\begin{aligned} \frac{1}{\alpha^*} &= \overline{\left(\frac{x_s(t) + y_s(t) + m(t)}{x_r(t) + y_r(t)}\right)} \\ &= \overline{\left(\frac{x_s(t) + y_s(t)}{x_r(t) + y_r(t)}\right)} + \overline{\left(\frac{m(t)}{x_r(t) + y_r(t)}\right)}, \end{aligned} \tag{10}$$

where $\overline{f(t)}$ denotes the temporal average of $f(t)$ over of a period T. In case $m(t)$ has zero mean, as in the example given in [14], the second term of Eq. (10) vanishes since $m(t)$ is independent of $x_r(t) + y_r(t)$, and the amplitude of $x_r(t) + y_r(t)$ is much larger than that of $m(t)$; while the first term of Eq. (10) reveals the approximate value of α^*. This simple procedure may be slightly inexact due to the divide-by-zero problem, so the low-amplitude samples were eliminated and the following algorithm was used to determine α^* with higher accuracy:

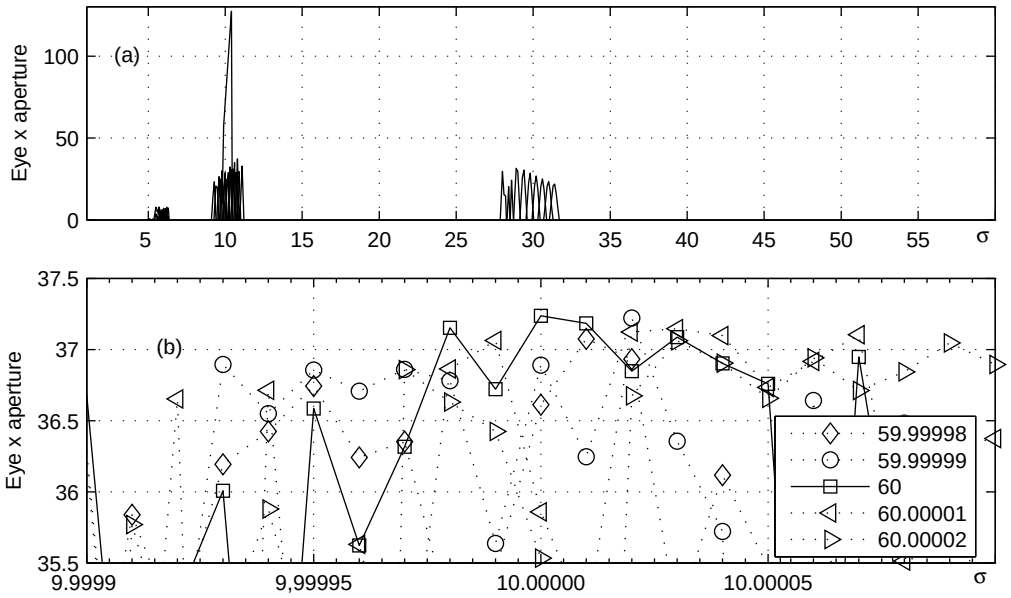

Figure 8: The eye aperture x_r of the intruder's receiver system for various measure periods: (a) 8 seconds, with $r^* = 59.8$ to $r^* = 60.2$; (b) 800 seconds, with $r^* = 59.9999$ to $r^* = 60.0001$.

1. select a collection of samples of $x_r(t)$ and $y_r(t)$, corresponding to the 800 first seconds of the waveform,
2. calculate the maximum value M_{x+y} of the collection of $|x_r(t) + y_r(t)|$ samples,
3. compile a list of all the exact sampling times t_j for which $|x_r(t_j) + y_r(t_j)| > 0.3\ M_{x+y}$ and count the number of them n_j,
4. calculate the scaling factor as $\alpha^* = \dfrac{1}{n_j} \sum_{j=1}^{n_j} \dfrac{x_r(t_j) + y_r(t_j)}{U(t_j)}$.

The result was $\alpha^* = 5.000038$ for all the four parameter sets previously identified, which represents a relative error of 7×10^{-6} related to α, that will affect the recovery of $m(t)$ by adding a negligible noise of 63 db below the amplitude of $m(t)$.

The retrieved plaintext then can be calculated as:

$$m^*(t) = U(t) - \frac{x_r(t) + y_r(t)}{\alpha^*} = x_s(t) + y_s(t) + m(t) - \frac{x_r(t) + y_r(t)}{\alpha^*} \tag{11}$$

Figure 9 illustrates the plaintext waveforms of the original message $m(t)$ and of the four recovered messages $m^*(t)$ between 799 and 800 seconds, for the four system parameter sets previously identified. It can be seen that the retrieved waveforms corresponding to the first and the second sets of the parameters of the intruder's receiver system are exactly equal to the waveform of the original plaintext. In comparison, for the third and fourth sets of parameters the retrieved plaintext has a small distortion. Note that the distortion increases as the eye aperture goes down, as can be expected. Nevertheless, any of the four potential candidates of the response system's parameter sets may be used indistinctly to gain access to the encrypted information without significant error, during the limited time period that was considered for their determination.

5. Generalizing the parameter determination method to other chaotic systems

The described parameter determination procedure, by means of the eye aperture maximization of a drive-response system, was also tested for other chaotic attractors with a scroll shape. We found that it was

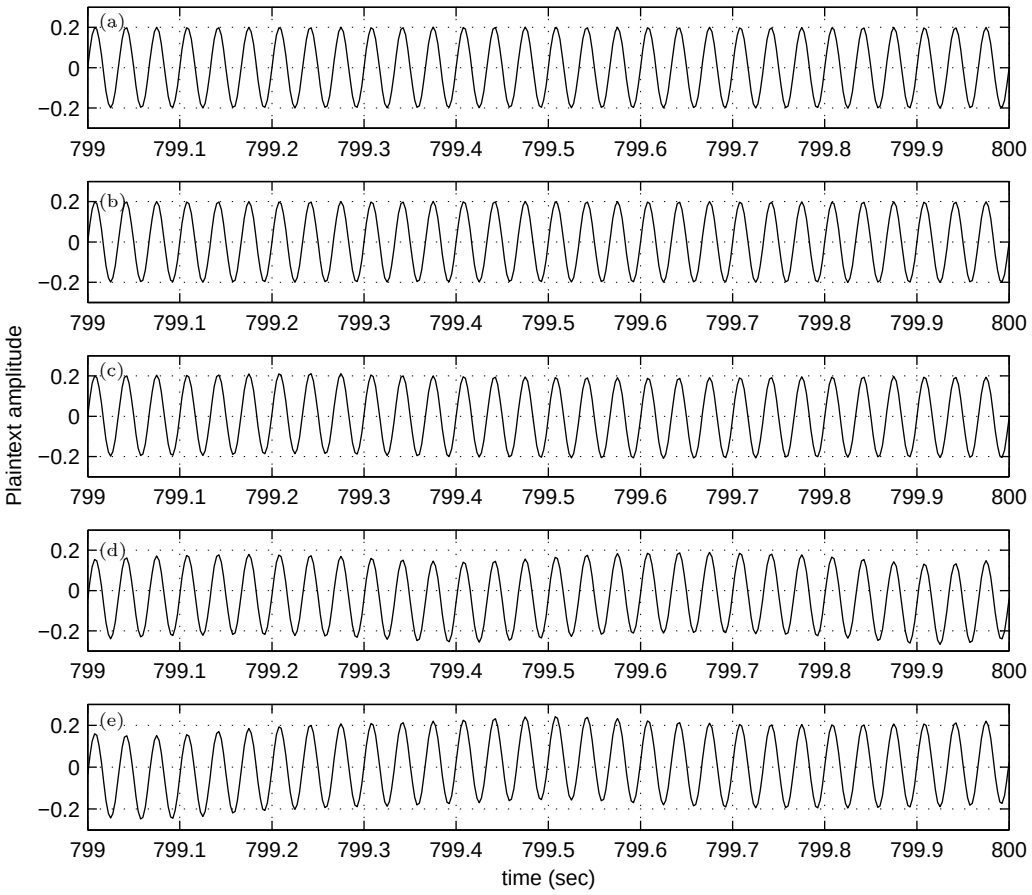

Figure 9: Last second of plaintext. (a) Original message. Retrieved plaintext for four sets of response system parameters: (b) $r_1^* = 60$, $\sigma_1^* = 10$; (c) $r_1^* = 59.99999$, $\sigma_1^* = 10.00002$; (d) $r_2^* = 60$, $\sigma_2^* = 10.00001$; (e) $r_3^* = 60$, $\sigma_3^* = 9.99998$.

not possible to apply it to the Rössler and the van der Pol-Duffing systems [31], but it works well for the Chua's circuit [32]. We believe that it could be also applied to some other chaotic systems generalized from the Chua's circuit and the Lorenz system such as those reported in [33, 34], and also applicable to other multi-torus chaotic attractors [35].

As an example, we present the application of this procedure to a drive-response system implemented with the Chua's circuit, which is defined in its dimensionless form by the following state equations:

$$\begin{aligned} \dot{x} &= a\left[m_1 x + y - h(x)\right], \\ \dot{y} &= x - y + z, \\ \dot{z} &= -by, \end{aligned} \tag{12}$$

where $h(x) = 0.5(m_1 - m_0)(|x+1| - |x-1|)$, and a, b, m_0, m_1 are the system's parameters.

The response system is defined by the following equations, in which the variable $y(t)$ is the driving signal received from the sender:

$$\begin{aligned} \dot{x_r} &= a^*\left[m_1^* x_r + y - h^*(x_r)\right], \\ \dot{z_r} &= -b^* y, \end{aligned} \tag{13}$$

where $h^*(x_r) = 0.5(m_1^* - m_0^*)(|x_r+1| - |x_r-1|)$, and a^*, b^*, m_0^*, m_1^* are parameters.

Figure 10 shows the double-scroll Chua's attractor formed by the projection on the x_r-y plane when three possible cases of parameter coincidence are considered. In Fig. 10(a), all common parameters of the drive and response systems are equal: $a = a^* = 9$, $b = b^* = 14.28$, $m_1 = m_1^* = 0.28$, $m_0 = m_0^* = -0.13$. It can be observed that the attractor's eye is quite open. In Fig. 10(b), three parameters coincide, but one differs: $m_0^* = -0.12 \neq m_0$, it can be seen that eye aperture has diminished compared with the former case. In Fig. 10(c), two parameters coincide, but the other two differ: $a^* = 9.1 \neq a$ and $m_0^* = -0.12 \neq m_0$. It can be seen that the eye is completely closed, i.e. the eye x_r-aperture is negative. In all cases the same initial conditions were used for both the drive and response system: $x(0) = x_r(0) = 0.25$, $z(0) = z_r(0) = 0.25$, $y(0) = -0.25$.

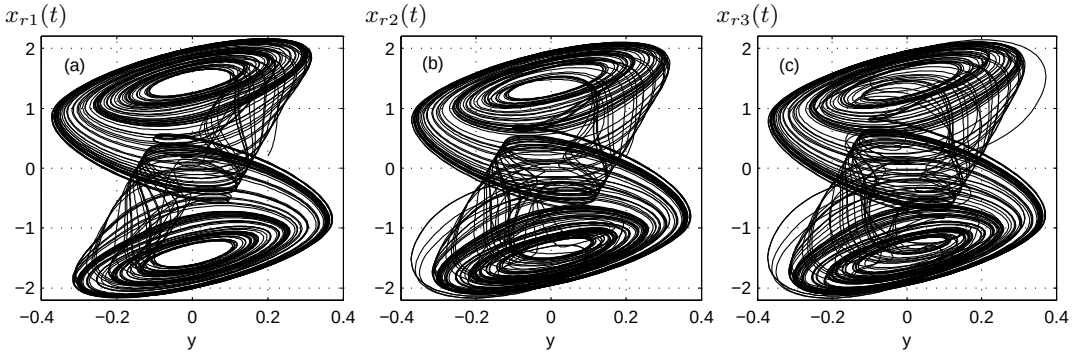

Figure 10: Chua's chaotic attractor formed by the projection on the x_r-y plane. The parameter of the drive system are the same for all the three cases: $a = 9$, $b = 14.28$, $m_1 = 0.28$, $m_0 = -0.13$. The parameters of the response system are: (a) $a^* = a$, $b^* = b$, $m_1^* = m_1$, $m_0^* = m_0$; (b) $a^* = a$, $b^* = b$, $m_1^* = m_1$, $m_0^* = -0.12$; (c) $a^* = 9.1$, $b^* = b$, $m_1^* = m_1$, $m_0^* = -0.12$.

6. Simulations

All results were obtained from simulations with MATLAB 7.6. The Lorenz integration algorithm was a four-fifth order Runge-Kutta with an absolute error tolerance of 10^{-9}. The relative error tolerance was 10^{-6}, and the sampling frequency was 400 Hz.

7. Conclusion

This work describes a novel parameter determination procedure of some double-scroll chaotic systems, based on the measure of some geometric properties of the chaotic attractor, with the help of a homogeneous driving synchronization mechanism. The method is applicable to the cryptanalysis of two two-channel chaotic cryptosystems that use the variable $z(t)$ as the synchronization signal, allowing for the system secret key recovery and evincing that such systems are not suitable for secure communications. The method is not applicable to break two-channel chaotic cryptosystems that use the variable $x(t)$ or $y(t)$ as the synchronization signal.

Acknowledgements

The authors are grateful to the anonymous reviewers for their valuable comments. The work described here was supported by Ministerio de Ciencia e Innovación of Spain, research grant MTM2008-02194 "CUCO" and by CDTI (Spain) in collaboration with Telefónica I+D, project SEGUR@ (CENIT 2007-2010). Shujun Li was supported by a fellowship from the Zukunftskolleg of the Universität Konstanz, Germany, which is part of the "Exzellenzinitiative" Program of the DFG (German Research Foundation).

References

[1] L. M. Pecora, T. L. Carroll. Synchronization in chaotic systems. Phys. Rev. Lett. 1990;64:821–4.
[2] T. Yang. A survey of chaotic secure communication systems. Int. J. Comput. Cognit. 2004;2:81–130.
[3] R. L. Devaney. A first course in chaotic dynamical systems. Reading, MA, USA: Addison-Wesley; 1992.
[4] M. Boutayeb, M. Darouach, H. Rafaralahy. Generalized state-space observers for chaotic synchronization and secure communication. IEEE Trans. Circuits Syst. I-Fundam. Theor. Appl. 2002;49(3):345–9.
[5] Q. Memon. Synchronized chaos for network security. Comput. Commun. 2003;26:498–505.
[6] S. Bowong. Stability analysis for the sinchronization of chaotic systems with different order: application to secure communication. Phys. Lett. A 2004;326(1-2):102–13.
[7] G. Alvarez, F. Montoya, M. Romera, G. Pastor. Breaking two secure communication systems based on chaotic masking. IEEE Trans. Circuits Systems II: Exp. Briefs. 2004;51(10):505–6.
[8] G. Alvarez, S. Li. Breaking network security based on synchronized chaos. Comput. Commun. 2004;27:1679–81.
[9] G. Alvarez, L. Hernandez, J. Muñoz, F. Montoya, S. Li. Security analysis of a communication system based on the synchronization of different order chaotic systems. Phys. Lett. A 2005;345(4-6):245–50.
[10] K. M. Short, Steps toward unmasking secure communications, Int. J. Bifurcat. Chaos 1994;4(4):959–77.
[11] K. M. Short. Detection of teleseismic events in seismic sensor data using nonlinear dynamic forecasting. Int. J. Bifurcat. Chaos 1997;7(8):1833–45.
[12] Z. P. Jiang. A note on chaotic secure communication systems. IEEE Trans. Circuits Syst. I-Fundam. Theor. Appl. 2002;49(1):92–6.
[13] B.-H. Wang, S. Bu. Controlling the ultimate state of projective synchronization in chaos: application to chaotic encryption. Int. J. Mod. Phys. B 2004;18(17-19):2415–21.
[14] Z. Li, D. Xu. A secure communication scheme using projective chaos synchronization. Chaos Solitons Fractals 2004;22:477–81.
[15] A. Kerckhoffs, La cryptographie militaire, Journal des sciences militaires 1883;IX(1,2):5–38,161–91.
[16] D. Stinson. Cryptography: theory and practice. Boca Raton, USA: CRC Press; 1995.
[17] E. N. Lorenz. Deterministic non periodic flow. J. Atmos. Sci. 1963;20(2):130–41.
[18] L. M. Pecora, T. L. Carroll. Driving systems with chaotic signals. Phys. Rev. A 1991;44:2374–83.
[19] R. Mainieri, J. Rehacek. Projective synchronization in three-dimensional chaotic systems. Phys. Rev. Lett. 1999;82(15):3042–5.
[20] D.Xu, Z. Li. Controlled projective synchronization in nonparametrically-linear chaotic systems. Int. J. Bifurcat. Chaos 2002;12(6):1395–402.
[21] T. Stojanovski, L. Kocarev, U. Parlitz. A simple method to reveal the parameters of the Lorenz system. Int. J. Bifurcat. Chaos 1996;6(12B):2645–52.
[22] U. Parlitz. Estimating model parameters from seriesby autosynchronization. Phys. Rev. Lett. 1996;76(8):1232–5.
[23] D. Huang. Synchronization based estimation of all parameters of chaotic systems fron time series. Phys. Rev. E 2004;69(6):067201.
[24] D. Yu, U. Parlitz. Estimating parameters by autosynchronization with dynamics restrictions. Phys. Rev. E 2008;77(6):066221.
[25] D. Yu, F. Liu. Dynamical parameter identification from a scalar time series. Chaos 2008;18(4):043108.
[26] A. B. Orue, V. Fernandez, G. Alvarez, G. Pastor, , M. Romera, S. Li, F. Montoya. Determination of the parameters for a Lorenz system and application to break the security of two-channel chaotic cryptosystems. Phys. Lett. A 2008;372(34):5588–92.
[27] G. Alvarez, S. Li, F. Montoya, M. Romera, G. Pastor. Breaking projective chaos synchronization secure communication using filtering and generalized synchronization. Chaos Solitons Fractals 2005;24(3):775–83.
[28] U. Parlitz, L. Junge, L. Kocarev. Synchronization-based parameter estimation from time series. Phys. Rev. E 1996;54(6):6253–9.
[29] K. M. Cuomo, A. V. Oppenheim. Circuit implementation of synchronized chaos with applications to communications. Phys. Rev. Lett. 1993;71(1):65–8.
[30] G. Alvarez, S. Li. Some basic cryptographic requirements for chaos-based cryptosystems. Int. J. Bifurcat. Chaos 2006;16(8):2129-51.
[31] J. Gutirrez, A. Iglesias. Syncronizing chaotic systems with positive conditional lyapunov exponents by using convex combinations of the drive and response systems. Phys. Lett. A 1998;239(3):174–80.
[32] L. Chua. A zoo of strange attractors from the canonical Chua's circuits. In: Proceedings of the 35th Midwest Symposium on Circuits and Systems. IEEE; 1992. vol. 2, p. 916–26.
[33] M. E. Yalcin, J. A. K. Suykens, J. Vandewalle. Families of scroll grid attractors. Int. J. Bifurcat. Chaos 2002;12(1):23–41.
[34] S. Yu, W. Tang, J. Lu, G. Chen. Design and implementation of multi-directional grid multi-torus chaotic attractors. IEEE Trans. Circuits Syst. I: Regul. Pap. 2008;55(11):1168–72.
[35] S. Yu, J. Lu, G. Chen. Design and implementation of multi-directional grid multi-torus chaotic attractors. IEEE Trans. Circuits Syst. I: Regul. Pap. 2006;54(9):2087–98.