Breaking a SC-CNN-based Chaotic Masking Secure Communication System*

AB. Orue, V. Fernandez, G. Alvarez, G. Pastor, M. Romera, F. Montoya
Instituto de Física Aplicada, CSIC
c/. Serrano 144, 28006 Madrid, Spain
fausto@iec.csic.es

C. Sanchez-Avila
DMAT, ETSI Telecomunicación, UPM, Madrid 28040, Spain

Shujun Li
FernUniversität in Hagen, Lehrgebiet Informationstechnik,
Universitätsstraße 27 - PRG, 58084 Hagen, Germany

Abstract

This paper studies the security of a chaotic cryptosystem based on Chua's circuit and implemented with State Controlled Cellular Neural Networks (SC-CNN). Here we prove that the plaintext can be retrieved by bandpass filtering of the ciphertext or by using an imperfect decoder with wrong receiver parameters. In addition we find that the key space of the system can be reduced notably, and the required resolution of the parameter values to recover a meaningful plaintext is as coarse as 5%, easing a brute-force attack. The system parameters can be determined with high precision through the analysis of the decoding error produced by the mismatch between the parameters of receiver and transmitter.

Keywords - Chua's attractor, cryptanalysis, chaotic masking.

1 Introduction

The possibility of synchronization of two coupled chaotic systems was first shown by Pecora & Carroll [1990, 1991]. Due to the nonpredictable behavior of chaotic variables, it was soon envisaged the possibility of using them in the field of secure communications in the same way as the white noise and random sequences were used in classical cryptography. Accordingly, a great number of cryptosystems based on chaos have been proposed [Cuomo & Oppenheim, 1993a,b; Wu & Chua, 1993; Lozi & Chua, 1993; Zhigang Li, 2004; Yang, 2004], some of them fundamentally flawed by a lack of robustness and security [Pérez & Cerdeira, 1995; Alvarez *et al.*, 2004b, 2005].

Chua's circuit [Chua, 1992] is a simple chaotic circuit generally considered to be the paradigm of chaos [Madan & Wu, 1993]. It is defined in its dimensionless form by the following state equations:

$$\begin{aligned} \dot{x} &= \alpha\left[y - h(x)\right], \\ \dot{y} &= x - y + z, \\ \dot{z} &= -\beta y - \gamma z, \end{aligned} \tag{1}$$

*This paper has been published in *International Journal of Bifurcation and Chaos*, vol. 19, no. 4, pp. 1329–1338, 2009.

with $h(x) = m_1 x + 0.5(m_1 - m_0)(|x+1| - |x-1|)$, where x, y and z are the system's variables; $\dot{x}$, $\dot{y}$ and $\dot{z}$, are the derivative of the variables with respect to time τ and α, β, γ, m_0 and m_1 are the system's parameters.

A particular implementation of Chua's circuit was introduced by Arena *et al.* [1995], using a State Controlled Cellular Neural Network (SC-CNN) formed by the suitable interconnection of three generalized CNN cells. Its dimensionless form is defined by the following state equations:

$$\begin{aligned} \dot{x}_1 &= -x_1 + s_{11}x_1 + s_{12}x_2 + a_1 y_1, \\ \dot{x}_2 &= -x_2 + s_{21}x_1 + s_{23}x_3, \\ \dot{x}_3 &= -x_3 + s_{32}x_2 + s_{33}x_3, \end{aligned} \tag{2}$$

where $y_1 = 0.5(|x_1 + 1| - |x_1 - 1|)$.

It can be seen that Eqs. (1) can be obtained from Eqs. (2) with $x_1 = x$, $x_2 = y$, and $x_3 = z$, whenever the following conditions hold: $a_1 = \alpha(m_1 - m_0)$; $s_{11} = 1 - \alpha\, m_1$; $s_{12} = \alpha$; $s_{21} = s_{23} = 1$; $s_{32} = \beta$; $s_{33} = 1 - \gamma$.

The advantage of the CNN cell model is that the implementation of the circuit can be achieved using off-the-shelf electronic components such as resistors, capacitors and operational amplifiers, unlike the original Chua's circuit, which needs to be built using *Chua's diode*, a special nonlinear negative resistance.

Recently, Kiliç *et al.* [2004] proposed a new chaotic cryptosystem by implementing Chua's circuit with the above SC-CNN technique. It was a chaotic masking system with feedback algorithm. This structure was originally proposed by Milanović & Zaghloul [1996] in order to obtain a robust synchronization between the transmitter and receiver of a communication scheme using a modified Lorenz chaotic system. The results of a PSpice simulation were presented by Kiliç *et al.* [2004] and a hardware implementation was later described in [Günay & Alçi, 2005]. The cryptosystem's transmitter was defined as (also in dimensionless form):

$$\dot{x}_1 = -x_1 + s_{11}x_1 + s_{12}x_2 + a_1 y_1, \tag{3}$$
$$\dot{x}_2 = -x_2 + s_{21}m(\tau) + s_{23}x_3, \tag{4}$$
$$\dot{x}_3 = -x_3 + s_{32}x_2 + s_{33}x_3, \tag{5}$$

where $m(\tau) = x_1(\tau) + s(\tau)$ is the ciphertext and $s(\tau)$ is the plaintext. It can be observed the ciphertext $m(\tau)$ feedback in the second equation of the system.

The cryptosystem's receiver was defined as:

$$\dot{x}'_1 = -x'_1 + s_{11}x'_1 + s_{12}x'_2 + a_1 y'_1, \tag{6}$$
$$\dot{x}'_2 = -x'_2 + s_{21}m(\tau) + s_{23}x'_3, \tag{7}$$
$$\dot{x}'_3 = -x'_3 + s_{32}x'_2 + s_{33}x'_3, \tag{8}$$

where $y'_1 = 0.5(|x'_1 + 1| - |x'_1 - 1|)$.

The recovered plaintext $s'(\tau)$ at the receiver's end was calculated as: $s'(\tau) = m(\tau) - x'_1(\tau)$.

In [Kiliç *et al.*, 2004] the following parameters were used: $\alpha = 9$, $\beta = 14 + \frac{2}{7}$, $\gamma = 0$, $m_0 = -\frac{1}{7}$, $m_1 = \frac{2}{7}$, $s_{21} = s_{23} = 1$, $s_{33} = 1 - \gamma = 1$. Note that these parameters correspond to the dimensionless form. In real circuit implementations, the time response (and also the spectrum) of the circuit is adjusted by changing the capacitor's value in each cell. According to the full circuit scheme of the SC-CNN-based chaotic masking system shown in Fig. 6 of [Kiliç *et al.*, 2004], the time-scale factor is $t/\tau = R_{24}C_{21}$, where t denotes the time associated with the real circuit implementation. In one of the PSpice experiments simulated in [Kiliç *et al.*, 2004], the values of the resistor $R_{24} = 100\mathrm{K}\Omega$ and the capacitor $C_{21} = 51\mathrm{nF}$, which leads to a time-scale factor $t/\tau = R_{24}C_{21} = 51 \times 10^{-6}$ (or $\tau/t = 10^6/51 \approx 19608$). This configuration was also used in the hardware realization in [Günay & Alçi, 2005] and was in fact the configuration used for all our experiments. Please note that the cryptanalysis' results reported in this paper apply similarly for different configurations.

The signal waveforms of the variable x_1, plaintext $s(t) = \sin(2\,\pi\,1000\,t)$, ciphertext and retrieved text in one of our experiments are illustrated in Fig. 1.

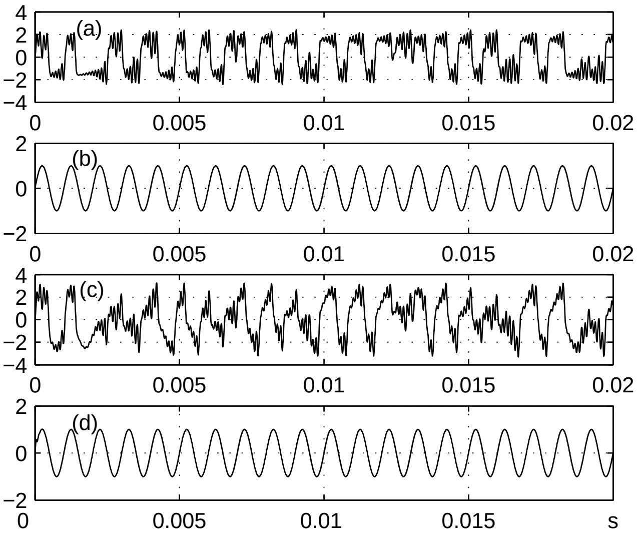

Figure 1: Waveforms from the example used in [Kiliç *et al.*, 2004] and [Günay & Alçi, 2005]: (a) Variable $x_1(t)$ of the transmitter; (b) plaintext $s(t) = \sin(2\,\pi\,1000\,t)$; (c) ciphertext $m(t) = x_1(t) + s(t)$; (d) retrieved plaintext at the receiver end $s'(t)$.

Figure 2 shows the double scroll Chua's attractor resultant from the projection in the phase space of a trajectory portion extending along 0.2 s on the (x_2, x_1) plane. The trajectory of Chua's attractor draws two 3D loops situated in the vicinity of the equilibrium points P^+ and P^-. This trajectory has the shape of a spiral, which grows steadily in amplitude and jumps from one of the equilibrium points to the other, at irregular intervals and in a random-like manner. The trajectory may pass arbitrarily near to the equilibrium points, but never reaches them while in chaotic regime. The two asterisks show the locations of the attractor's equilibrium points, of coordinates $x_{1P^\pm} = \pm(1 - \frac{m_0}{m_1})$, $x_{2P^\pm} = 0$, $x_{3P^\pm} = \mp(1 - \frac{m_0}{m_1})$ [Chua, 1992].

In Fig. 3 the frequency power spectrum of the transmitter's variable $x_1(t)$ is depicted, showing that most of the energy is located at the band below 2 kHz. This energy corresponds to the higher amplitude and slow oscillations of $x_1(t)$, associated to the jumps between the two loops. There is a notable peak at the position of the plaintext frequency $f = 1000$ Hz, which is due to the presence of $m(\tau)$ in Eq. (4). There are also some power components of higher frequency around 8kHz, as a consequence of the small amplitude ripple of $x_1(t)$, associated to the turns around the equilibrium points.

The rest of the paper is organized as follows. In Sec. 2 several weaknesses of the cryptosystem are analyzed. In Secs. 3 and 4 different ways to break this cryptosystem such as filtering and brute-force attack are also shown. Finally Sec. 5 presents the conclusions and final remarks.

2 Problems With the Cryptosystem's Definition

Although the authors of [Kiliç *et al.*, 2004] and [Günay & Alçi, 2005] seemed to base the security of their cryptosystem on the chaotic behavior associated with the output of Chua's circuit, neither analysis of security, nor indications about key selection, nor allowable plaintext frequency, nor amplitude and system initial conditions were included.

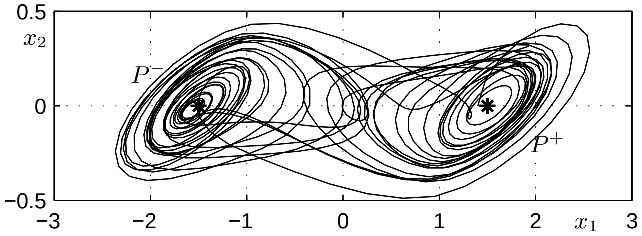

Figure 2: Trajectory of Chua's atractor projected onto the (x_2, x_1) plane.

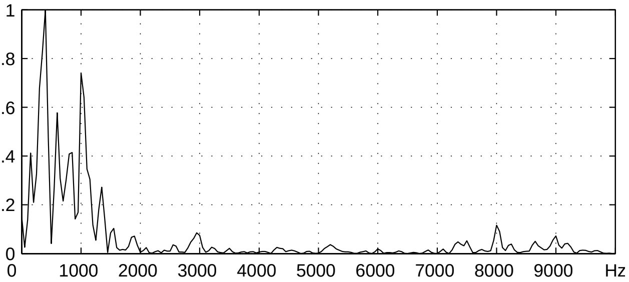

Figure 3: Relative power spectrum of the $x_1(t)$ transmitter's variable.

2.1 Missing key specification

The first issue to be considered in a cryptosystem is the secret key. A cryptosystem cannot exist without a key. When cryptanalyzing a cryptosystem the assumption commonly made is that the cryptanalyst knows exactly the design and functioning of the cryptosystem under study, i.e., he knows every detail about the ciphering algorithm, but he does not posses any information about the secret key. This is an evident requirement in today's secure communications systems, usually referred to as Kerckhoffs' principle [Alvarez & Li, 2006]. In [Kiliç *et al.*, 2004; Günay & Alçi, 2005] none of the following issues were considered: the necessity of a key in the proposed system, what this should consist of, the available key space (how many different keys exist in the system), the precision to be used, and how this should be created and managed. None of these elements should be neglected when describing a secure communication system [Alvarez & Li, 2006; Alvarez *et al.*, 2004a].

A typical assumption made by most chaotic cryptosystems' designers is that the system's parameters play the role of the key [Alvarez *et al.*, 2005]. Such premise will be assumed throughout the rest of the article.

2.2 Dangerous initial conditions and forbidden operation regions

It is a well known fact that for the parameter values of the example given in [Kiliç *et al.*, 2004; Günay & Alçi, 2005], there are many unstable periodic orbits embedded in the double scroll attractor [Madan & Wu, 1993, Table B1]. If for any reason during the operation of the system some specific points are reached, or these are included in the initial conditions, the system becomes unstable with ever-growing amplitude of the variables. Such points must be considered as forbidden during normal operation.

The system proposed by Kiliç *et al.* [2004] and Günay & Alçi [2005] differs from the traditional Chua's circuit in its strong feedback scheme. Hence it may be conjectured whether the forbidden regions hold or have disappeared. The stability of some known conflicting points was assessed. Some of them were no longer unstable, although others remained unstable such as $\{x_1(0), x_2(0), x_3(0)\} = \{1.83487,\ 0,\ 2.53784\}$, and, far worse, the existence of a complete forbidden region of the attractor's orbit and/or initial conditions, corresponding to the values $x_2 \geq 1.08$ - for any value of x_1 and x_3 - was observed.

This problem does not involve a security threat, but it will degrade the reliability of the communication system. Hence, attention must be paid to detect it during operation in order to apply the appropriate corrective measures.

2.3 Dangerous plaintexts

In Kiliç *et al.* [2004] it was claimed that plaintext signals of 1 V to 2 V of amplitude did not disturb the chaos synchronization. An example was illustrated using plaintext signals with sinusoid and triangle waveforms of 1 kHz of frequency and 1 V of amplitude.

As the plaintext is fed into the transmitter's Eq. (4), the normal behavior of Chua's circuit is disturbed. The higher the amplitude of $s(t)$, the more serious the disturbance becomes. It was found that all the variables of the attractor remained synchronized with the plaintext, for plaintexts of 1 V of amplitude and frequencies ranging from about 4700 Hz to 4970 Hz.

This is a very dangerous situation as the ciphertext reveals the plaintext. For frequencies comprised between 4970 Hz and 12500 Hz, an unstable periodic orbit of about 9500 Hz is reached, which makes the system not operable for plaintexts with frequencies from 4700 Hz to 12500 Hz and an amplitude of 1 V. Furthermore it was found that for amplitudes as high as 2 V this frequency band spans from 3200 Hz to 14300 Hz. To ensure the circuit's orbit remains as a double scroll for any plaintext frequency it was found that its amplitude should remain less than 0.24 V.

Speech signals have an spectrum whose maximum amplitude takes place at approximately 1000 Hz, decaying very fast with increasing frequencies, to the point of having low power density at frequencies higher than 3200 Hz and no power density at frequencies higher than 5000 Hz. Therefore it can be concluded that the system, using the settings of the example of [Kiliç *et al.*, 2004], is suitable for the encryption speech signals, but not for other signals having a spectrum of high amplitude at frequencies higher than 3200 Hz.

3 Breaking the System by Filtering

The main problem associated with the cryptosystem under study consists in the synchronization mechanism between transmitter and receiver, which is excessively robust. The consequence is that for a given transmitter parameter set an almost correct synchronization can be reached for a very large number of inexact receiver parameter combinations.

A necessary condition for any cryptosystem to be secure is that the system's parameters that play the role of the key are sensitive enough to guarantee that if a plaintext encrypted with one particular key k_1 is decrypted with a wrong key k_2 differ dramatically from the plaintext decrypted with the right key, thus concealing any information about the plaintext ([Alvarez & Li, 2006]). In other words, the normalized cross-correlation coefficients between the plaintext and the recovered text using all the possible wrong keys should have zero value, or very close to zero.

Unfortunately the proposed cryptosystem does not fulfill this requirement. On the contrary, given a ciphertext encrypted with a specific parameter set k_1, it is possible to find an empirical formula, which allows us to find a large quantity of distinct receiver parameter sets - completely different from k_1 - that enable the decryption and almost exact recovery of the plaintext, via band-pass filtering it.

Figure 4 shows the value of the maximum cross-correlation coefficient between the original plaintext and the band-pass filtered recovered plaintext, decrypted with various values of $\alpha' \neq \alpha$. The filter used was a finite impulse response digital band-pass filter, with 200 taps and a frequency response range of 300 Hz to 3400 Hz, which is the typical bandwidth of telephone loops. The plaintext was a pure tone of 1000 Hz. The values of the receiver's parameters were chosen according to an empirical recipe as follows: α' was freely chosen, while the rest of them were chosen as a function of α', such as $\beta' = \alpha' + 5.3$, $m_0' = \frac{\pi}{100} - \frac{\pi}{2\alpha'}$

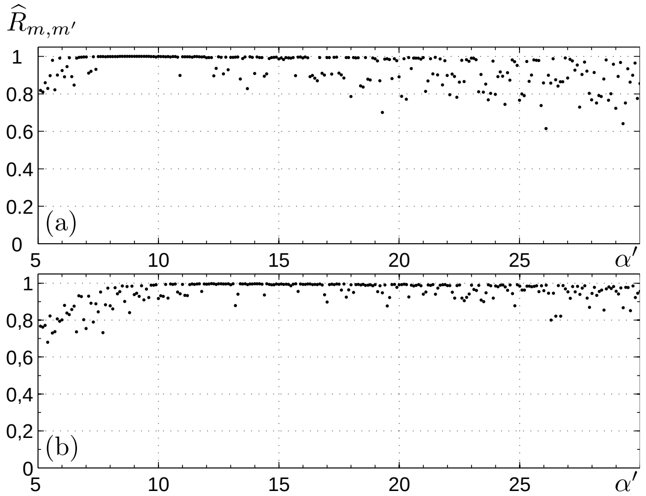

Figure 4: Maximum cross-correlation coefficient $\widehat{R}_{m,m'}$ between the plaintext m and the filtered recovered text m' for various sets of wrong decryption keys: (a) transmitter's parameters of the example in [Kiliç *et al.*, 2004] $\alpha = 9$, $\beta = 14 + \frac{2}{7}$, $m_0 = -\frac{1}{7}$, $m_1 = \frac{2}{7}$; (b) arbitrary transmitter's parameters $\alpha = 12$, $\beta = 18$, $m_0 = -\frac{3}{25}$ and $m_1 = \frac{1}{4}$.

and $m'_1 = \frac{\pi}{\alpha'} - \frac{\pi}{50}$. Two cases are presented, the case (a) corresponds to the values of the transmitter's parameters of the example in [Kiliç *et al.*, 2004]. Case (b) corresponds to a different arbitrary chosen set of values of the transmitter's parameters within the valid range: $\alpha = 12$, $\beta = 18$, $m_0 = -\frac{3}{25}$ and $m_1 = \frac{1}{4}$.

It can be seen that for a great majority of the 250 trials of the α' parameter, in each case, the maximum cross-correlation coefficient between the plaintext and the filtered recovered text with wrong key has a value nearly equal to unity, i.e. the plaintext is recovered without neither noise nor distortion. For the remaining trials the maximum normalized cross-covariance coefficient has a value above 0.6, which means this is a good approximation, yet not perfect, of the plaintext. Therefore any information that should be hidden by the proposed cryptosystem could be compromised.

Figure 5 illustrates the problem step by step. The signals of the system corresponding to the values of the transmitter's parameters: $\alpha = 9$, $\beta = 14 + 2/7 \approx 14.2857$, $m_0 = -1/7 \approx -0.1429$, $m_1 = 2/7 \approx 0.2857$; and an arbitrary set of values of the receiver's parameters, chosen sufficiently separated from those of the transmitter's: $\alpha' = 17$, $\beta' = 23.3$, $m'_1 = 0.1366$, $m'_0 = -m'_1/2 = -0.0683$ are depicted. The plaintext was $s(t) = \sin(2\,\pi\,1000\,t)$.

It can be appreciated that the waveform of the receiver's chaotic variable $x'_1(t)$ resembles pretty much that of the transmitter's $x_1(t)$. Hence the retrieved plaintext $s'(t)$ differs from the original plaintext $s(t)$ mainly in the higher frequency components, i.e. the jumps between the equilibrium points are alike, but not the rate and amplitude of turns around them, which causes a high frequency noise on the retrieved plaintext. This noise can be easily removed by filtering. Figure 5(f) shows the recovered plaintext after being filtered using the same digital bandpass filter used in the experiments shown in Fig. 4.

4 Breaking the System by brute-force Attack

One possible way to break the system is by a *brute-force attack*, which consists of trying all the possible values of its parameters until a meaningful and noise-free plaintext is obtained [Alvarez & Li, 2006, Sec. 4.4].

However a brute-force attack will only be feasible in the case of a small key space. Thus, to prevent it, the number of possible keys should be as large as possible. Nowadays the veteran Data Encryption Standard is considered obsolete and was abandoned since it *only* has $2^{56} = 7.2 \times 10^{16}$ different keys. In fact, provided today's computing power, the size of the key space is recommended to be at least 2^{100} to resist these type

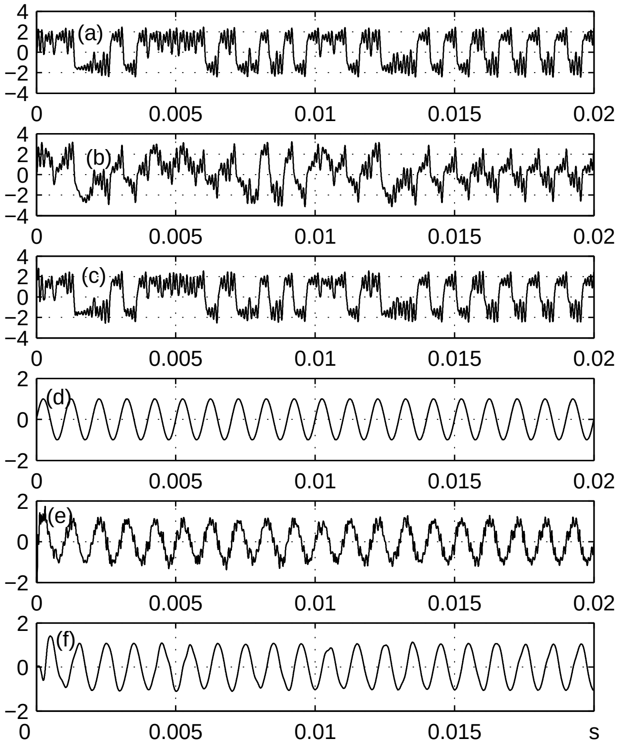

Figure 5: Plaintext retrieved with wrong parameter guessing: (a) Chaotic variable of the transmitter $x_1(t)$; (b) ciphertext $m(t) = \; x_1(t) + s(t)$; (c) chaotic variable of the receiver $x'_1(t)$; (d) plaintext $s(t) = sin(2\,\pi\,1000\,t)$; (e) retrieved plaintext $s'(t)$; (f) bandpass-filtered retrieved plaintext $s'(t)$.

of attacks.

4.1 Reduced hypothetical key space

The problem associated with using Chua's circuit as a cryptosystem is that the useful range for the parameter's values becomes quite reduced. In [Matsumoto, 1987; Madan & Wu, 1993] it is shown that Chua's circuit exhibits almost every known bifurcation and chaotic phenomenon described in the literature. Its manifold is quite complex, which is why it is known as the chaos paradigm. Different combinations of parameters α and β lead to many different trajectories projected onto the (x_2, x_1) plane. Among them are: double-scroll strange attractor, sinks, asymmetric periodic orbits, period-n orbits, Rössler like spiral, heteroclinic orbits, homoclinic orbits and repulsive foci. The only attractor behavior suitable for masking the plaintext is the double-scroll attractor, since other behaviors give place to very simple waveforms that cannot hide the plaintext in an efficient manner. Unfortunately, the region of the (α, β) plane giving rise to the double-scroll attractor is a small fraction of about 4% of all possible combinations of parameter values, as shown in [Matsumoto, 1987; Madan & Wu, 1993]. Hence a hypothetical key space based on the system's parameters would be much smaller than initially expected.

This situation is worsened by the fact that some parameters of Chua's circuit have a direct relation with the coordinates x_1 of the attractor's equilibrium points P^+ and P^-, that can be approximately delimited by observing the ciphertext waveform. This further reduces the key space, as will be later described.

As the system described in [Kiliç *et al.*, 2004] and [Günay & Alçi, 2005] differs from the ordinary Chua's circuit in the fact that it makes use of feedback, it may have a different behavior from that of the ordinary one. Therefore the region of the (α, β) plane giving rise to the double-scroll attractor was experimentally investigated for different combinations of the remaining parameters m_0 and m_1. The results are depicted in Fig. 6. Depending on the values of m_0 and m_1 the points within this region may or may not cause a double scroll attractor. However the points outside this region never cause a double scroll attractor for any combination of m_0 and m_1 values. Therefore they are not suitable for hiding information and need not to be investigated when mounting a brute-force attack. The region that must be investigated is approximately delimited by the curves $\beta = 0.0062\,\alpha^2 + 0.92\,\alpha + 0.5$ and $\beta = 0.157\,\alpha^2 - 0.16\,\alpha + 12$. Hence the usable key space is notably reduced.

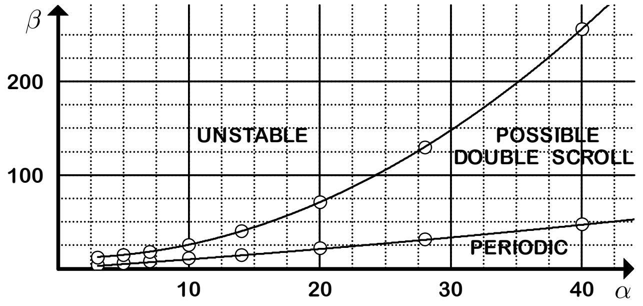

Figure 6: Region of the (α, β) plane giving rise to the double-scroll attractor.

Correspondingly, the region of the (m_0, m_1) plane giving rise to the double-scroll attractor may also be delimited from Chua's circuit definition and from the ciphertext as follows.

According to the definition of Chua's circuit, the parameters m_0 and m_1 are $m_0 = (G_a/G) + 1$ and $m_1 = (G_b/G) + 1$, where G is a positive conductance while G_a and G_b are the two negative conductances of the equivalent circuit of the Chua's nonlinear resistor. They satisfy the relation $G_a < G_b < 0$, hence it follows that $1 > m_1 > m_0$. If the coordinates of the attractor's equilibrium points $x_{1P^\pm} = \pm(1 - \frac{m_0}{m_1})$ could be determined, a tighter relationship between m_0 and m_1 could be established.

If the undisturbed chaotic variable of the transmitter $x_1(t)$ was accessible, the coordinates $x_{1P^\pm} = \pm(1 - \frac{m_0}{m_1})$ of the equilibrium points $P^\pm$ could be determined from the variable waveform. Figure 7 (a) shows the waveform of $x_1(t)$ and the true values of x_{1P^+} and x_{1P^-}. As can be seen it is not a difficult task to approximate the value of x_{1P^+} or x_{1P^-} as the equidistant line between the relative maxima and minima of the positive or negative part, respectively, of the waveform $x_1(t)$.

However, as the only accessible data to an opponent cryptanalyst is the ciphertext $m(t) = x_1(t) + s(t)$ – depicted in Fig. 7 (c)) – the transmitter's variable $x_1(t)$ remains obscured by the presence of the plaintext. Consequently only a coarse estimation of $x_{1P^\pm}$ can be attained. Nevertheless the value may be delimited effectively by establishing two easily measurable bounds. As $x_{1P^+} = -x_{1P^-}$, it is preferable to work with the absolute value of $m(t)$, represented in Fig. 7 (d). The value of $|x_{1P^\pm}|$ can be delimited between the bounds $x_{1\max}$ and $x_{1\text{mean}}$, being the former the maximum value of $|m(t)|$ and the later the mean of $|m(t)|$. It is evident from Fig. 7 (d) that $|x_{1P^\pm}| < x_{1\max}(t)$ and it was found experimentally – for a large assortment of parameter values and plaintexts – that in all cases $|x_{1P^\pm}| > x_{1\text{mean}}(t)$. The true value of $\frac{m_0}{m_1}$ corresponds to -0.5. Hence$|x_{1P^\pm}| = 1 - \frac{m_0}{m_1} = 1.5$, which is in good agreement with the bounds that were experimentally found: $x_{1\max} = 3.00$ and $x_{1\text{mean}} = 1.41$. This allows for an important reduction of the search range of the possible values of m_0 and m_1. As $x_{1\max} = 3.00 > \pm(1 - \frac{m_0}{m_1}) > x_{1\text{mean}} = 1.41$ and $1 > m_1 > m_0$, it follows that:

$$1 > m_1 > 0 \text{ and } -0.41 m_1 > m_0 > -2m_1,$$

resulting in the key space being additionally reduced.

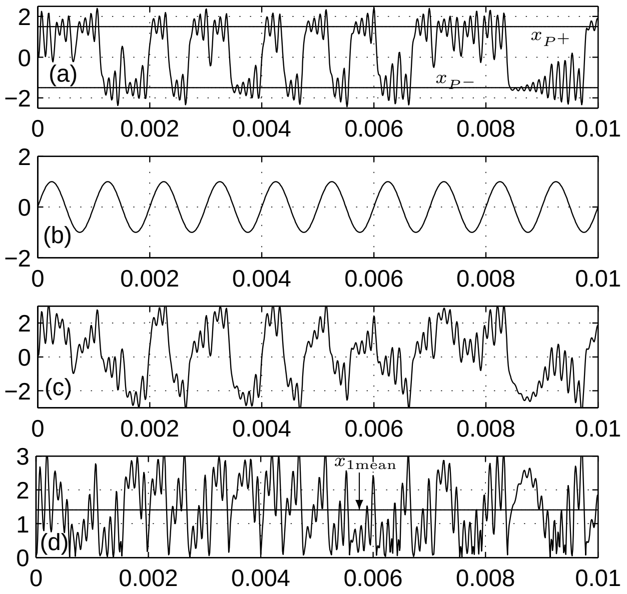

Figure 7: Estimation of the equilibrium points : (a) transmitter's chaotic variable $x_1(t)$ with x_{1P^+} and x_{1P^-}; (b) plaintext $s(t)$; (c) ciphertext $m(t) = x_1(t) + s(t)$; (d) absolute value of ciphertext $|m(t)|$.

4.2 Required key precision

Establishing the required precision of the proposed cryptosystem's key is the critical point to withstand a brute-force attack. In a perfect cryptosystem a message encrypted using a specific key should not be vulnerable to an intent of decryption with a different key even if they both differ in the minimum possible amount allowed by machine precision [Alvarez & Li, 2006, Rule 9].

The problem of the system under study consists in the low precision required to define the decryption key, which consequently makes the number of effectively different keys very small too. Figure 8 illustrates this problem, showing the retrieved plaintext for three sets of values for the receiver's parameters α', β', m_0', m_1', different from the transmitter's parameters α, β, m_0, m_1. As can be seen, the plaintext is almost perfectly retrieved for a guessing error of 1% in the magnitude of each receiver's parameter. The initial error is due to the transitory caused by the different initial conditions between transmitter and receiver. Furthermore an error as high as 5% still produces a recognizable retrieved plaintext.

The best brute-force attack strategy consists of trying all possible keys using a coarse parameter resolution of ±5%, beginning by the most probable values and subsequently expanding the search area if a satisfactory result is not reached. Once the best set of parameter values is found, the precision of these parameters is to be refined to find those that provide the 'cleanest' recovered plaintext.

With a reduced resolution of ±5% the number of required trials is limited to 24 parameter values to cover a decade of variation of the parameter[1]. Initially the value of the α parameter may be searched in the range between 4 and 40, while the value of m_1 may be searched between 0.05 and 0.5. Using the limits for β and m_0 established in the Sec. 4.1, the total number of trials will be approximately $390,000 \approx 2^{18.6}$, which constitutes a modest number of keys. In case of failure, the search space should be progressively broadened.

[1] The same rule is used by hardware makers to define the nominal values of electronic components, for instance the resistor series of ±5% precision is covered with 24 values. I.e.: the first value should be 1, it covers from 0.95 till 1.05, the second 1.1 that will cover from 1.05 to 1.15, the third 1.1^2 and so on, with 24 steps the total covered margin will be from 0.95 to $1.1^{24} = 9.84$, as described in IEC 60062 norm

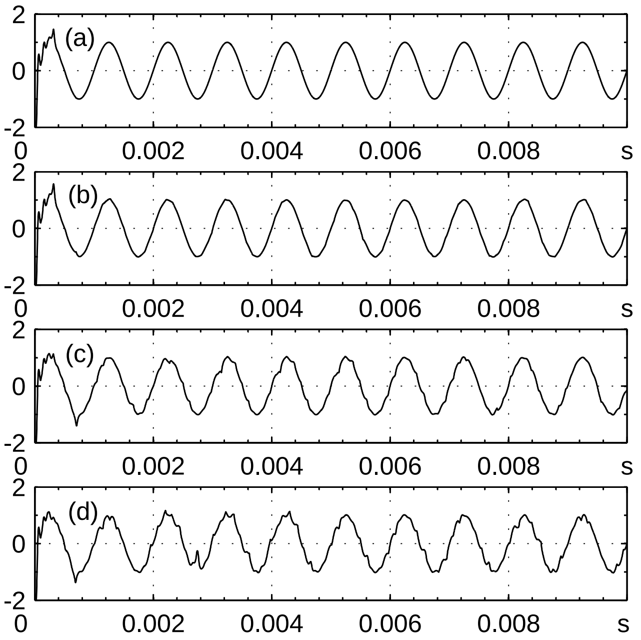

Figure 8: Plaintext retrieved with slightly wrong parameter guessing: (a) retrieved plaintext with $\{\alpha',\ \beta',\ m_0',\ m_1'\} = \{\alpha,\ \beta,\ m_0,\ m_1\}$; (b) retrieved plaintext with $\{\alpha',\ \beta,'\ m_0',\ m_1'\} = 1.01 \times \{\alpha,\ \beta,\ m_0,\ m_1\}$; (c) retrieved plaintext with $\{\alpha',\ \beta,'\ m_0',\ m_1'\} = 0.97 \times \{\alpha,\ \beta,\ m_0,\ m_1\}$; (d) retrieved plaintext with $\{\alpha',\ \beta,'\ m_0',\ m_1'\} = 1.05 \times \{\alpha,\ \beta,\ m_0,\ m_1\}$.

4.3 Parameter determination

As illustrated in Fig. 3, the transmitter's variable $x_1(t)$, which acts as a noise to mask the plaintext, has two well differentiated frequency bands. The lower frequency band has spectral components generally lower than 3 kHz, which correspond to the jumps of the attractor between the two loops centered at the equilibrium points P^+ and P^-. This part effectively conceals the plaintext characterized with the same frequency band. The second one constitutes a higher frequency band, located near 8 kHz, associated with the loops of the attractor's trajectory around the equilibrium points.

If the ciphertext was decrypted by an unauthorized receiver with wrong parameter guessing, it can be found that the retrieved plaintext $s'(t) = m(t) - x_1'(t) = s(t) + x_1(t) - x_1'(t)$ is composed by both the plaintext and the decoding error $\varepsilon = x_1(t) - x_1'(t)$, which can be considered as an unwanted masking noise. If the parameters of sender and receiver were equal, the decoding error would disappear. Consequently a strategy to retrieve the plaintext may consist of determining the receiver's parameters that minimize the decoding error. However, since the noise and the plaintext share the lower frequency band of the spectrum, their complete separation is not possible. However it is still possible to separate the higher frequency band from the decoding error. Therefore the plaintext should have a frequency spectrum limited to lower frequencies and sufficiently separated from the higher frequency band of the noise.

Figure 9 illustrates the relative power spectrum of the receiver decoding error. The lower frequency components are mixed with the plaintext whereas the higher frequency components are far from the plaintext frequencies. Therefore the decoding error created by the higher frequencies of ε can be easily extracted from the ciphertext by means of a high-pass filter with a cut-off frequency of 6.5 kHz, in order to reject the plaintext frequencies and retain the higher frequency components of the noise.

Figure 10 illustrates the logarithm of the power for the higher frequency components of the decoding error ε for different sets of the receiver's parameters α', m_1' and m_0' as a function of β'. It can be seen that the minimum decoding error is reached when the parameters of both the transmitter and receiver agree. All the

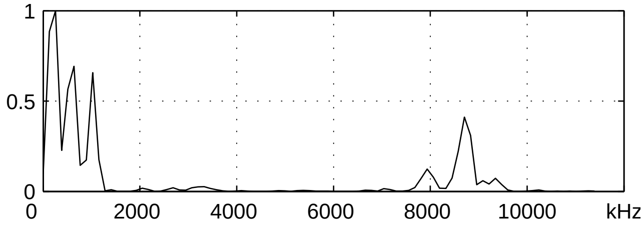

Figure 9: Relative power spectrum of the receiver decoding error ε, with transmitter parameters: $\alpha = 9$, $\beta = 14 + 2/7 \approx 14.2857$, $m_0 = -1/7 \approx -0.1428$, $m_1 = 2/7 \approx 0.2857$; and arbitrarily chosen receiver's parameters: $\alpha' = 4.5$, $\beta' = 9$, $m_0' = -0.12$, $m_1' = 0.21$.

curves show the same tendency: the decoding error grows with the mismatch between the transmitter's and receiver's parameters. Moreover their relative minima is reached for values close to those of the transmitter's.

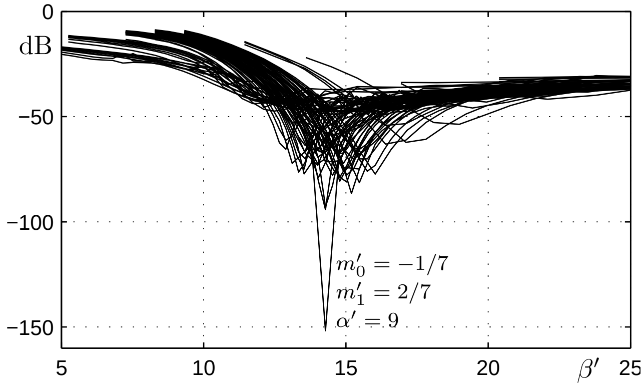

Figure 10: Power of the higher frequency components of the decoding error ε, for different sets of values of the receiver's parameters: $\alpha' = \{4, \ldots, 20\}$; $m_1' = \{0.01, \ldots, 0.9\}$; $m_0' = \{0.01, \ldots, 1.8\}$.

An iterative optimization procedure consisting of a number of approximation rounds in order to determine the parameter values that gave rise to the minimum decoding error was developed. In each round the four parameters were varied one at a time, starting from a set of arbitrary values $\alpha' = 5$, $\beta' = 7$, $m_1' = 0.1$, $m_0' = 0.2$. In total 31 values of each parameter were tried within the limited range defined in Sec. 4.1 and the value giving rise to the lowest decoding error was retained. During each successive round the margin of variation of each parameter was progressively reduced. The procedure was ended when a fixed value of the parameters was reached. The number of required rounds for this to happen was 30 and the elapsed computing time was 965 seconds (on a PC with a 4 GHz Pentium Dual CPU). Figure 11 illustrates the story of the procedure, showing the variation of each parameter as a function of the round number. The values of the parameters were determined with a precision from five to six significant digits, allowing for the exact retrieving of the plaintext.

5 Conclusion

The secure communication system described in [Kiliç *et al.*, 2004; Günay & Alçi, 2005] was studied. It was found that the synchronization mechanism is excessively robust with the consequence that an almost exact synchronization can be reached for an infinite number of combinations of the receiver's parameters. Therefore the plaintext can be retrieved by simple band-pass filtering after decoding the ciphertext with a receiver with wrong parameters, or by direct filtering of the ciphertext.

It was also found that the key space of the system can be notably reduced by means of the study of the

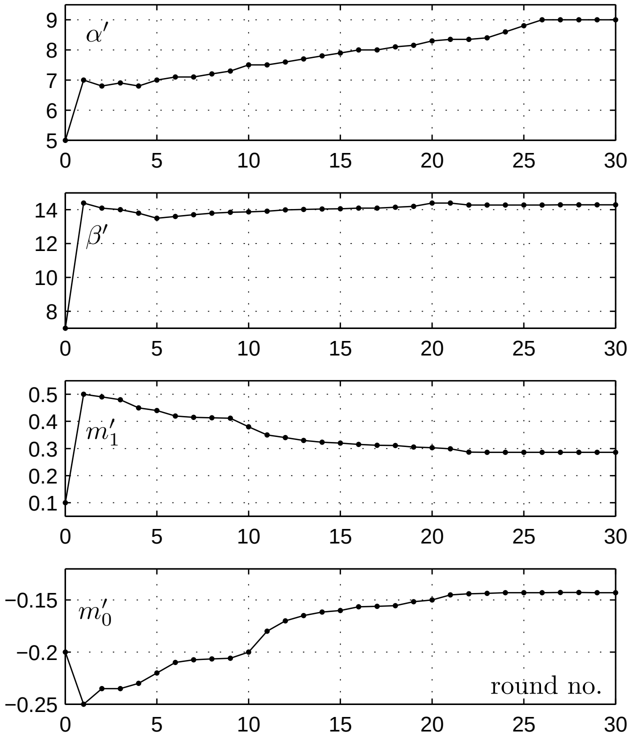

Figure 11: Story of the approximation followed by the parameters' value.

geometric properties and the chaotic regions of Chua's attractor. The required resolution of the parameter values to recover a meaningful plaintext is as coarse as 5%. Hence a brute-force attack is fully feasible.

Finally, the parameters of the system were determined with high precision, by analyzing and minimizing the decoding error created by the mismatch between the parameters of receiver and transmitter.

It must be concluded that the cryptosystem described in [Kiliç *et al.*, 2004] and [Günay & Alçi, 2005] is not secure and must be not used for sensible data protection.

Acknowledgment

This work was supported by *Ministerio de Ciencia e Tecnologìa* of Spain, research grant TSI2007-62657. Shujun Li was supported by a research fellowship from the Alexander von Humboldt Foundation, Germany.

References

Alvarez, G. & Li, S. [2006] "Some basic cryptographic requirements for chaos-based cryptosystems," *Int. J. Bifurc. Chaos* **16**, 2129–2151.

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

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

Alvarez, G., Montoya, F., Romera, M. & Pastor, G. [2004b] "Breaking parameter modulated chaotic secure communication system," *Chaos Solitons Fractals* **21**, 783–787.

Arena, P., Baglio, S., Fortuna, L. & Manganaro, G. [1995] "Chua's circuit can be generated by CNN cells," *IEEE Trans. Circuits Syst. I* **42**, 123–125.

Chua, L. O. [1992] "The genesis of Chua's circuit" *Arch. für Elektron. & Übertrag.-tech.* **46**, 250–257.

Cuomo, K. M. & Oppenheim, A. V. [1993a] "Chaotic signals and systems for communications," in *Proc. IEEE Int. Conf. Acoustics, Speech, and Signal Processing (ICASSP'93)* **3** 137–140.

Cuomo, K. M. & Oppenheim, A. V. [1993b] "Circuit implementation of synchronized chaos with applications to communications," *Phys. Rev. Lett.* **71**, 65–68.

Günay, E. & Alçi, M. [2005] "Experimental confirmation of SC-CNN based chaotic masking systema with feedback," *Int. J. Bifurc. Chaos* **15**, 4013–4018.

Kiliç, R., Alçi, M. & Günay, E. [2004] "A SC-CNN based chaotic masking system with feedback," *Int. J. Bifurcat. Chaos* **14**, 245–256.

Lozi, R. & Chua, L. O. [1993] "Secure communications via chaotic synchronization. II. noise reduction by cascading two identical receivers," *Int. J. Bifurc. Chaos* **3**, 1319–1325.

R. N. Madan and C. W. Wu, "Introduction to experimental chaos using Chua's cirucit," in Chua's circuit: A paradigm for Chaos (R. N. Madan, ed.), pp. 59-89, Singapore: World Scientific, 1993.

Matsumoto, T. [1987] "Chaos in electronics circuits," *Proc. IEEE* **75**, 1033–1057.

Milanović, V. & Zaghloul, M. E. [1996] "Improved masking algorithm for chaotic communications systems," *Electron. Lett.* **32**, 11–12.

Pecora, L. M. & Carroll, T. L. [1990] "Synchronization in chaotic systems," *Phys. Rev. Lett.* **64**, 821–824.

Pecora, L. M. & Carroll, T. L. [1991] "Driving systems with chaotic signals," *Phys. Rev. A* **44**, 2374–2383.

Pérez, G. & Cerdeira, H. A. [1995] "Extracting messages masked by chaos," *Phys. Rev. Lett.* **74**, 1970–1973.

Wu, C. W. & Chua, L. O. [1993] "A simple way to synchronize chaotic systems with applications to secure communication systems," *Int. J. Bifurc. Chaos* **3**, 1619–1627.

Yang, T. [2004] "A survey of chaotic secure communication systems," *Int. J. Comput. Cogn.* **2**, 81–130.

Zhigang Li, D. X. [2004] "A secure communication scheme using projective chaos synchronization," *Chaos Solitons Fractals* **22**, 477–481.