ELSEVIER

31 August 1998

Physics Letters A 245 (1998) 495-510

PHYSICS LETTERS A

Cryptanalyzing chaotic secure communications using return maps

Tao Yang [a,1], Lin-Bao Yang [b], Chun-Mei Yang [c,d]

[a] *Electronics Research Laboratory and Department of Electrical Engineering and Computer Sciences, University of California at Berkeley, Berkeley, CA 94720, USA*
[b] *University of E-Zhou, E-Zhou, 436000, Hubei, China*
[c] *China Construction Bank Songjiang Sub-Branch, 201611 Shanghai, China*
[d] *Everbeauty Houseware (Shanghai) Co. Ltd., 201612 Shanghai, China*

Received 12 january 1998; revised manuscript received 1 May 1998; accepted for publication 8 May 1998
Communicated by C.R. Doering

Abstract

In chaotic secure communications, message signals are scrambled by chaotic dynamical systems. The interaction between the message signals and the chaotic systems results in changes of different kinds of return maps. In this paper, we use return map based methods to unmask some chaotic secure communication systems; namely, chaotic shift keying (chaotic switching), chaotic parameter modulation and non-autonomous chaotic modulation. These methods are used without knowing the accurate knowledge of chaotic transmitters and without reconstructing the dynamics or identifying the parameters of chaotic transmitters. These methods also provide a criterion of deciding whether a chaotic secure communication scheme is secure or not. The effects of message signals on the changes of different return maps are studied. Fuzzy membership functions are used to characterize different kinds of changes of return maps. Fuzzy logic rules are used to extract message signals from the transmitted signal. The computer experimental results are provided. The results in this paper show that the security of chaotic secure communication not only depends on the complexity of the chaotic system but also depends on the way the message is scrambled. A more complex chaotic system is not necessary to provide a higher degree of security if the transmitted signal has simple and concentrated return maps. We also provide examples to show that a chaotic system with complicated return maps can achieve a higher degree of security to the attacks presented in this paper. © 1998 Elsevier Science B.V.

PACS: 05.45.+b
Keywords: Chaotic cryptanalysis; Return map; Chaos; Chua's circuit; Chaotic secure communication; Fuzzy mathematics

1. Introduction

Recently, chaotic cryptography has become a very active research area. This is not strange if one considers that the cores of the classical cryptography; namely, the key generators for stream cipher are actually discrete chaotic (or pseudo-chaotic) dynamical systems. However, cryptology consists of two parts [1]: cryptography and cryptanalysis. Cryptography is the study of the methods and tools by which a message signal can be concealed in ciphers and later recovered by authorized users. Then for the intruder

[1] E-mail: taoyang@fred.eecs.berkeley.edu.

PII S0375-9601(98)00425-3

it is either impossible or computationally infeasible to recover the message signal without the secret key. On the other hand, cryptanalysis is the study of recovering a message signal from ciphers without knowing the secrete key. In classical cryptology, the cryptography is a systematic science with well-established analytical and synthetic principles and the cryptanalysis is rather like an art depending heavily on intuition and experience than a science.

Also, chaotic cryptography has been developed rapidly in recent years while chaotic cryptanalysis is still at its beginning with very few results littered among a huge ocean of chaotic cryptography literature [2–8]. But it is very necessary to develop chaotic cryptanalysis because the security of a chaotic cryptography scheme can not be measured by classical cryptography. We need to develop chaotic cryptanalysis which functions as the inner motivation of the further study of chaotic cryptography. Also, we need to provide criteria for judging the degree of security of chaotic cryptography. While classical cryptography can also be used in chaotic cryptography [9], the classical cryptanalysis can not be used in chaotic cryptanalysis, thus it should be a long way to go before developing efficient methods of chaotic cryptanalysis. In this paper we present some return map based cryptanalysis methods.

There exist many chaos-based secure communication schemes. Almost all these schemes need two identical chaotic systems; namely, a *chaotic transmitter* and a *chaotic receiver*. In the chaotic transmitter a message signal denoted by $m(t)$ is scrambled and then a signal from the transmitter, which may be the scrambled message signal or another state variable in the transmitter, called a *transmitted signal*, $s(t)$, is transmitted to the chaotic receiver. The synchronization between the chaotic transmitter and the chaotic receiver is usually needed to recover chaotic key signals. Then an inverse process is used to recover the message signal. The security of chaotic secure communication depends on the sensitivity of chaotic systems to their parameters and initial conditions. The previous work always assumes that it should be very difficult for the intruder to reconstruct the dynamics of the transmitter from the transmitted signal. And the identification of parameters of the transmitter gives such big errors that the intruder can not find the message signal.

The above assumptions may be true in certain cases, e.g., a very high dimensional hyper-chaotic transmitter. However, when an intruder wants to discover the message signal, does he need to reconstruct the dynamics of the transmitter? Since there is a big redundancy in both the chaotic transmitted signal and the message signal, in certain cases, the intruder does not need any knowledge of the transmitter. In Ref. [6], the average frequency difference between two attractors was used to unmask the chaotic shift keying. In Ref. [3], the authors found that there existed some small shifts in return maps when the transmitter worked in different attractors. Then the small shifts were used to recover the message signal from chaotic shift keying and additive masking. In Ref. [7], the authors found that a nonlinear filtering process could unmask chaotic shift keying even from hyper-chaotic carriers. In all the above schemes, the precise knowledge and the dynamics of the transmitters were not used. There are at least two kinds of redundancies in the transmitted signal that can be used. One is the amplitude information and the other is the frequency information. Although one of them is enough to recover the message signal successfully as those presented in Ref. [6], we find that the combination of them will give more accurate results.

There also existed some other chaotic cryptanalysis methods which were based on the reconstruction of the dynamics of transmitter from the transmitted signal [4,5,2]. The results in Ref. [4] for the first time showed that chaotic additive modulation was not secure given that the chaotic carrier was not complex enough. The result in Ref. [5] was also a very original one for breaking chaotic parameter modulation. Some adaptive synchronization schemes can also be used as the identification based cryptanalysis methods [8], which need partial knowledge of the transmitter.

Since chaotic secure communication schemes need to scramble message signals in their transmitters, message signals change the attractors of the transmitters. In this paper, we use return maps to detect these changes. Since the changes may be in both amplitude and frequency, two kinds of return maps are constructed and studied. Then the chaotic cryptanalysis problem is converted to the classification problem of return maps. Since the relation between the message signal and the changes of return maps is very complicated, we use fuzzy mathematical methods to interpret the changes in return maps.

The methods proposed in this paper can also be used as criteria of judging the degree of security of chaotic secure communications. The chaotic secure communication schemes whose return maps are more complicated or the changes of return maps are more irregular should have a higher degree of security.

The organization of this paper is as follows. In Section 2, characteristics of different return maps are studied when different message signals are scrambled using different chaotic scrambling methods. In Section 3, fuzzy mathematical methods are used to represent return maps which are constructed from insufficient samples. The fuzzy membership functions of return maps are used to decode message signals from chaotic shift keying and chaotic parameter modulation. In Section 4, the non-autonomous chaotic modulations with naked and compound transmitted signals are decoded. In Section 5, the unmasking performance of our methods are tested under the conditions of complicated return maps. In Section 6 we give our conclusions.

2. Characteristics of return maps

Different return maps of a chaotic transmitted signal can reveal the amplitude and frequency information of a message signal. The redundant information in the transmitted signal can be used to recover the message signal even though one can not find the exact parameters of the transmitter. This fact was first reported in Ref. [3], in which a kind of amplitude return map was used. In many cases, only amplitude return maps are not enough to detect message signals. We also need some return maps which can reveal frequency information. Our results are based on the systematic studies of two kinds of return maps.

In this paper, all the results are based on Chua's circuit [10], whose state equation is given by

$$\frac{dv_1}{dt} = \frac{1}{C_1}[G(v_2 - v_1) - f(v_1)],$$
$$\frac{dv_2}{dt} = \frac{1}{C_2}[G(v_1 - v_2) + i_3],$$
$$\frac{di_3}{dt} = \frac{1}{L}(-v_2 - R_0 i_3), \tag{1}$$

where $f(v_1)$, the piece-wise linear v-i characteristic of the Chua's diode, is given by

$$f(v_1) = G_b v_1 + \tfrac{1}{2}(G_a - G_b)(|v_1 + E| - |v_1 - E|), \tag{2}$$

where E is the breakpoint voltage of the Chua's diode.

Suppose that the state voltage v_1 is the transmitted signal, we study the return maps of v_1 under different conditions. From v_1 we can construct different kinds of return maps. Let $t_n^{\max}$ be the moment when $v_1(t)$ gets its nth local maximum $V_{\max}(n)$, and $t_n^{\min}$ be the moment when $v_1(t)$ gets its nth local minimum $V_{\min}(n)$. Let $T_{\max}(n) = t_n^{\max} - t_{n-1}^{\max}$ and $T_{\min}(n) = t_n^{\min} - t_{n-1}^{\min}$ be two time intervals, then we define the following return maps:

$$r_{\max}^A : V_{\max}(n) \mapsto V_{\max}(n+1), \tag{3}$$
$$r_{\min}^A : V_{\min}(n) \mapsto V_{\min}(n+1), \tag{4}$$
$$r_{\max}^T : T_{\max}(n) \mapsto V_{\max}(n), \tag{5}$$
$$r_{\min}^T : T_{\min}(n) \mapsto V_{\min}(n). \tag{6}$$

In this paper, we show that the following chaotic secure communications are not very secure if the return map based unmasking methods are used. The first one is called *chaotic parameter modulation*, which consists of *chaotic shift keying* [11] and chaotic parameter modulation [12]. These schemes use message signals to modulate (change) the parameters of chaotic transmitters such that the transmitters work in different chaotic attractors. Although shapes and statistical properties of these attractors are very similar, their return maps are subjected to changes which are big enough to reveal the message signals.

Another chaotic secure communication scheme uses message signals to drive chaotic transmitters such that the autonomous transmitters become non-autonomous systems [13](henceforth called *non-autonomous modulation*). It was hoped that the chaotic dynamics of the transmitters may conceal message signals. Although the message signals are scrambled by the dynamics (or structure) of the chaotic transmitters, which are supposed to be very sensitive to parameters and initial conditions, the distortion of the attractor caused by message signals can be used by return map based attacks to recover the message signal.

We first study the changes of different return maps when different massage signals are embedded. In this paper, we choose the following parameters as the *standard parameters*: C_1 = 17 nF, C_2 = 178 nF, G =

1 mS, $L = 12$ mH, $R_0 = 20\ \Omega$, $G_a = -1.139$ mS, $G_b = -0.711$ mS, $E = 1$ V. Chua's circuit exhibits a Rössler-like attractor for these parameters.

Fig. 1a shows two $r^A_{\max}$ maps for two different parameter sets. Black points show the $r^A_{\max}$ map of Chua's circuit with the standard parameters. The grey points show the $r^A_{\max}$ map with the same parameters as the standard ones except for $C_1 = 18$ nF and $L = 13$ mH (henceforth called the *second parameter set*). We can see that there exists a small shift and some structural differences between these two $r^A_{\max}$ maps. The fact that the majority of the points in both $r^A_{\max}$ maps are concentrated in the vicinity of some 1D curves gives us the possibility of distinguishing them even if there only exist some small parameter changes. If the return map is too scattered then it is difficult to distinguish the changes in the attractors because the two return maps are mixed and overlapped. The return maps $r^A_{\min}$, as shown in Fig. 1b, are examples of this kind of scattered return map. Also, black points show the return map of the standard parameters and the grey points show that of the second parameter set. Since there is this scattered property, both of the return maps are heavily mixed.

Since $r^A_{\max}$ and $r^A_{\min}$ can reveal the amplitude information of attractors, any change in the sizes of the attractors causes shifts or some structural deformations in these return maps. On the other hand, the changes of the parameters not only change the sizes of the attractors but also their natural frequencies. This fact was first used to decode chaotic shift keying by Yang [6]. In this paper, we will generalize the method presented in Ref. [6] by using two time-related return maps. Figs. 1c and 1d show $r^T_{\max}$ and $r^T_{\min}$, respectively. We can see that the black points and the grey points are concentrated in the vicinity of some vertical lines. The little horizontal shifts between black lines and grey lines denote the changes in natural frequency. One can also find some vertical shifts between the black lines and the grey lines. We do not use these vertical shifts because they only represent the size changes of attractors as shown in Figs. 1a and 1b.

The characteristics of return maps shown in Fig. 1 are useful to decode chaotic parameter modulations. To decode the non-autonomous modulation, we should study the changes of return maps when a message signal (outer force) is added into the chaotic system. A typical non-autonomous modulation in a Chua's circuit is given by [13]

$$\begin{aligned}\frac{\mathrm{d}v_1}{\mathrm{d}t} &= \frac{1}{C_1}[G(v_2 - v_1) - f(v_1 + m(t))],\\ \frac{\mathrm{d}v_2}{\mathrm{d}t} &= \frac{1}{C_2}[G(v_1 - v_2) + i_3],\\ \frac{\mathrm{d}i_3}{\mathrm{d}t} &= \frac{1}{L}(-v_2 - R_0 i_3),\end{aligned} \tag{7}$$

where $m(t)$ is the message signal and outer force.

In Fig. 2, the return maps of Chua's circuit in Eq. (7) with standard parameters and two different message signals are shown. $r^A_{\max}$, $r^A_{\min}$, $r^T_{\max}$ and $r^T_{\min}$ are shown in Figs. 2a, 2b, 2c and 2d, respectively. From Fig. 2a we can see that there exist some diagonal shifts between these two return maps. Unlike these return maps in Fig. 1a between which there exist some shape deformations because the changes of parameters can introduce some structural changes in attractors, those return maps only have a shift to each other and keep the same shape because the small message signal does not change the structure of the attractor significantly[2]. From Fig. 2b we can see that the message signal introduces a significant diagonal shift between these two return maps. Also, the shapes and sizes are not significantly changed. Since the message signal is injected into Chua's diode, the nature frequencies of the attractors are not significantly changed. We do not find any significant horizontal shifts in Figs. 2c and 2d.

3. Decoding chaotic parameter modulation

There exist two kinds of chaotic parameter modulation schemes: one is chaotic shift keying [11] for scrambling digital signals, the other is parameter modulation [12] for scrambling analogue signals. In this section we study the security of both schemes which are subjected to the return map based attacks.

[2] We have found that when the message signal is big enough, there exist some significant structural changes in the attractor. In chaotic secure communication, the structural changes of attractors should be avoided because they introduce significant differences.

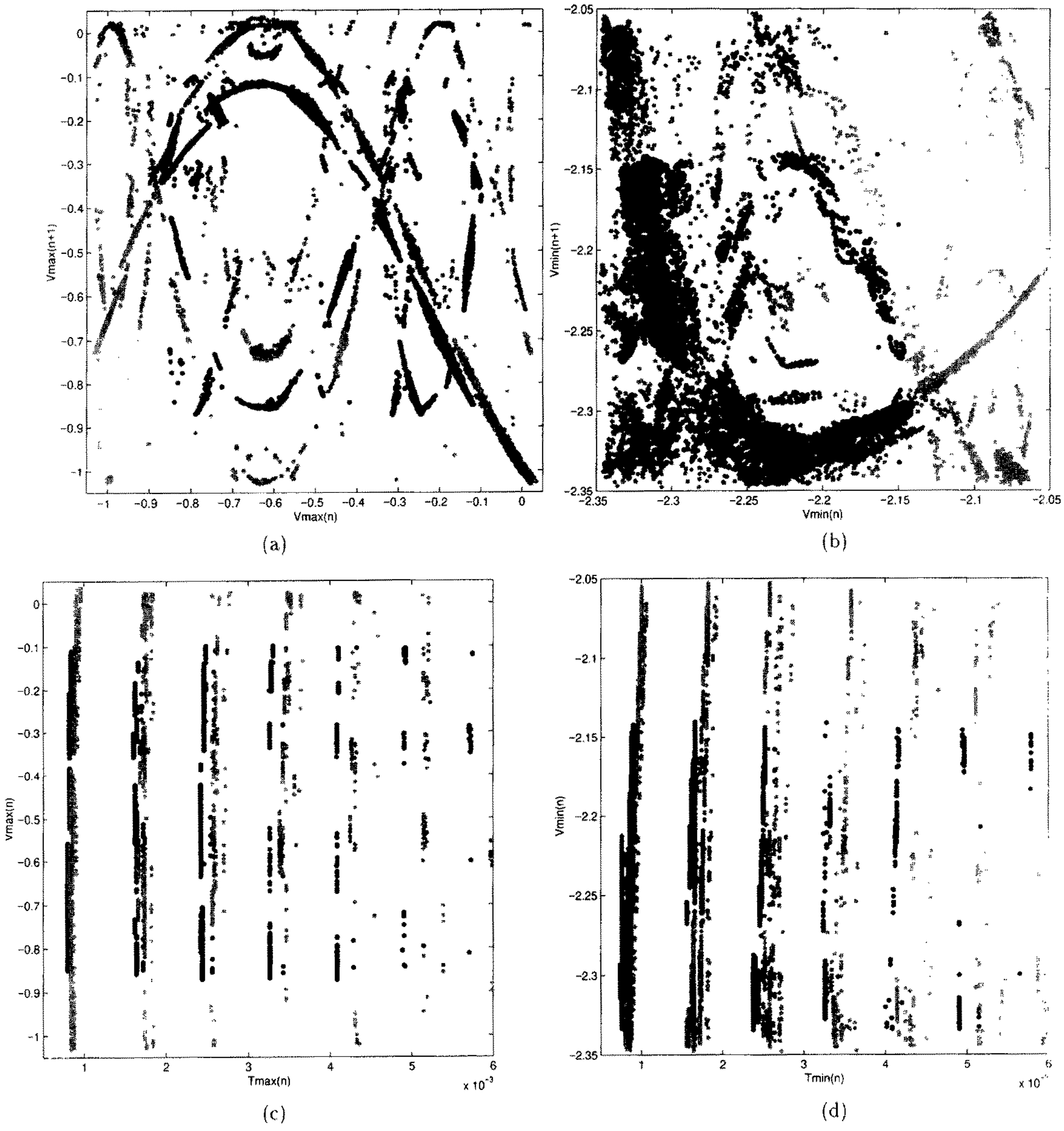
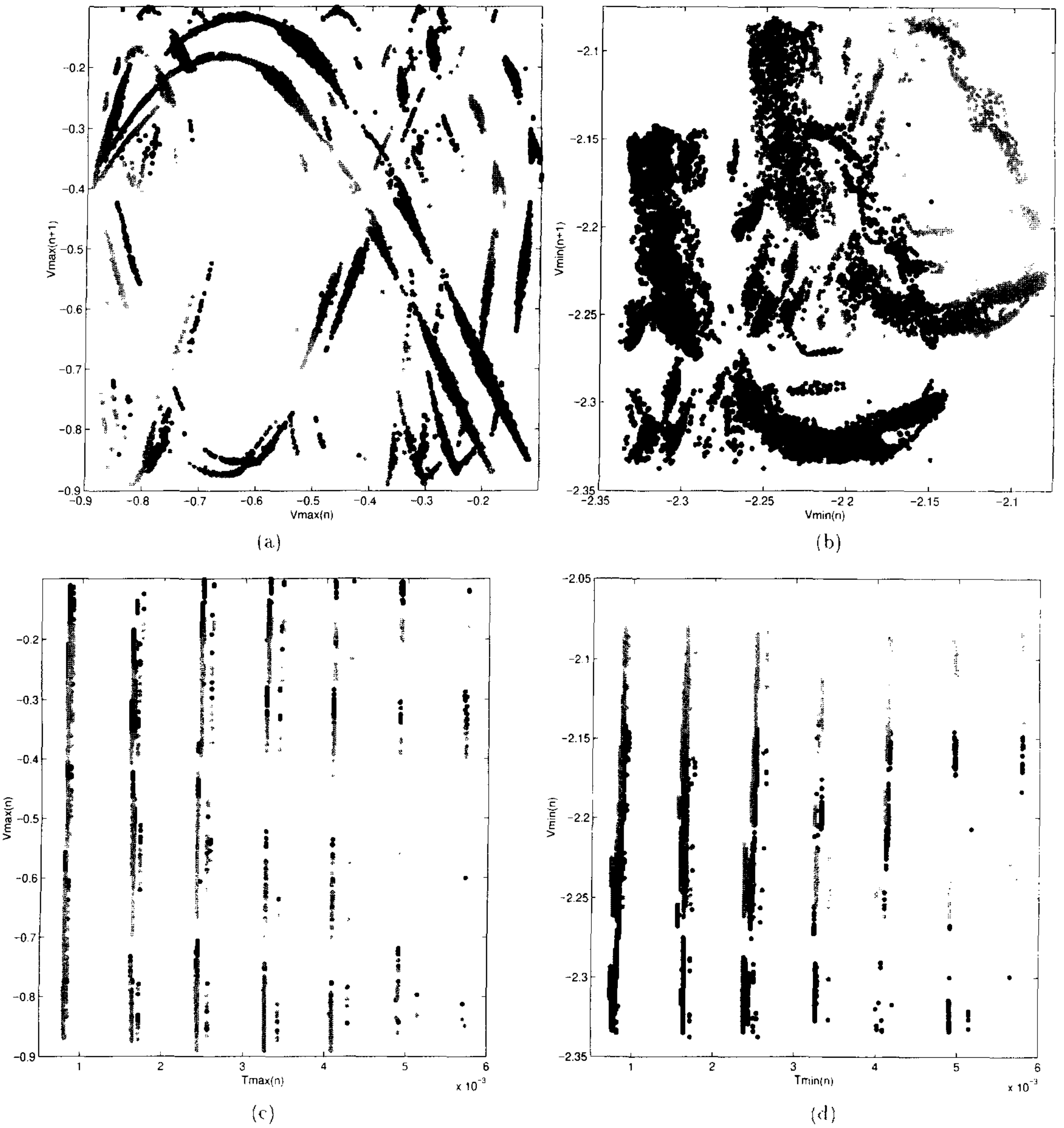


Fig. 1. The return maps of Chua's circuits with the standard parameter set and the second parameter set. Chua's circuits have Rössler-like attractors. The black points show the return maps of the standard parameter set and the grey points show the return maps of the second parameter set. (a) $r^A_{\max}$, (b) $r^A_{\min}$, (c) $r^T_{\max}$, (d) $r^T_{\min}$.

3.1. Security of chaotic shift keying

In chaotic shift keying [11], a binary information signal, $m(t)$, is encoded into two sets of parameters of the chaotic transmitter (i.e., two different chaotic attractors). At the receiver, $m(t)$ is decoded by synchronization errors, which are used to decide whether the received signal corresponds to one set of parameters or the other. In this paper, we choose the standard parameter set to denote digit "1" and the second parameter set to denote digit "0".

Assume that we have two-second records of $v_1(t)$



(a) (b)

(c) (d)

Fig. 2. The return maps of Chua's circuits with the standard parameter set and two different message signals when non-autonomous modulation is used. Chua's circuits have Rössler-like attractors. The black points show the return map of $m(t) = 0$ and the grey points show the return map of $m(t) = 0.01$ V. (a) $r^A_{\max}$, (b) $r^A_{\min}$, (c) $r^T_{\max}$, (d) $r^T_{\min}$.

with the standard parameters to construct the return maps. Since two-second records of $v_1(t)$ can not represent all the details of the return maps, there exist uncertainties due to the lack of data. Then the fuzziness arises from the insufficient data. On the other hand, since the return maps of different parameter sets may be so close that they partially overlay or mix with each other. The boundaries between return maps should be fuzzy. Suppose from these two-second samples of $v_1(t)$ we construct a standard return map $r^A_{\max} = \{V_{\max}(n), V_{\max}(n+1)\}^N_{n=1}$, which contains N points. Assume that we find a point (x, y) from the same return map of a transmitted signal $s(t)$ embedded with an unknown message signal $m(t)$, we then use the following membership value to denote the similarity between (x,y) and a point $(V_{\max}(n), V_{\max}(n+1))$ in the standard return map

$$\mu_{(V_{\max}(n),V_{\max}(n+1))}(x,y) = \max\left(0, 1 - \frac{(x-V_{\max}(n))^2+(y-V_{\max}(n+1))^2}{\alpha}\right),$$
$$n = 1,2,\dots,N, \tag{8}$$

where α is a small positive number. We call $\mu_{(V_{\max}(n),V_{\max}(n+1))}(x,y)$ the membership function of the following fuzzy linguistic statement:

"point (x,y) is the point $(V_{\max}(n), V_{\max}(n+1))$."

For those readers who are not familiar with fuzzy mathematics [14], $\mu_{(V_{\max}(n),V_{\max}(n+1))}(x,y)$ can be simply viewed as a kind of "distance" between points (x,y) and $(V_{\max}(n), V_{\max}(n+1))$.

Since $r^A_{\min}$ is useless for the tasks in this section, we do not assign a membership value to it. From Fig. 1c we can see that the return map $r^T_{\max}$ consists of vertical line segments and the significant changes of this map are along the horizontal direction, the membership function in this case is given by

$$\mu_{T_{\max}(n)}(t) = \max\left(0, 1 - \frac{|t-T_{\max}(n)|}{\beta}\right),$$
$$n = 1,2,\dots,K, \tag{9}$$

where β is a small positive number. We suppose that there are K points in the standard return map $r^T_{\max} = \{T_{\max}(n), V_{\max}(n)\}^K_{n=1}$, which is also constructed from the two-second samples. Also, $\mu_{T_{\max}(n)}(t)$ is the membership function of the following fuzzy linguistic statement:

"point t is the point $T_{\max}(n)$."

Similarly, the membership function of $r^T_{\min}$ is given by

$$\mu_{T_{\min}(n)}(t) = \max\left(0, 1 - \frac{|t-T_{\min}(n)|}{\gamma}\right),$$
$$n = 1,2,\dots,L, \tag{10}$$

where γ is a small positive number.

After setting the membership functions of the return maps with the standard parameters (henceforth called *standard return maps*), we observe the transmitted signal $s(t)$ and compare the difference between its return maps and the standard return maps. We use a membership value $\mu_1(s(t))$ to denote the degree of the similarity between the transmitter and Chua's circuit with the standard parameter set (henceforth called *standard transmitter*) with respect to $r^A_{\max}$. $\mu_1(s(t))$ is given by

$$\mu_1(s(t)) = \max_{n=1}^{N} \mu_{V_{\max}(n),V_{\max}(n+1)}(V^*_{\max}(i), V^*_{\max}(i+1)),$$
$$t \in [t^{\max}_{i+1}, t^{\max}_{i+2}), \tag{11}$$

where $V^*_{\max}(i)$ is the ith maximum value of $s(t)$. The fuzzy interpretation of Eq. (11) is the degree of the truth of the following fuzzy linguistic rule:

"If $(V^*_{\max}(i), V^*_{\max}(i+1))$ is $(V_{\max}(1), V_{\max}(2))$,
OR if $(V^*_{\max}(i), V^*_{\max}(i+1))$ is $(V_{\max}(2), V_{\max}(3))$,
OR $\cdots$
OR if $(V^*_{\max}(i), V^*_{\max}(i+1))$
is $(V_{\max}(N), V_{\max}(N+1))$,
THEN $(V^*_{\max}(i), V^*_{\max}(i+1))$ belongs to the
standard return map $r^A_{\max}$."

Similarly, we use $\mu_2(s(t))$ to denote the degree of similarity between the transmitter and the standard transmitter with respect to $r^T_{\max}$ and $\mu_3(s(t))$ to denote that with respect to $r^T_{\min}$, then we have

$$\mu_2(s(t)) = \max_{n=1}^{K} \mu_{T_{\max}(n)}(T^*_{\max}(i)),$$
$$t \in [t^{\max}_{i}, t^{\max}_{i+1}), \tag{12}$$

$$\mu_3(s(t)) = \max_{n=1}^{L} \mu_{T_{\min}(n)}(T^*_{\min}(i)),$$
$$t \in [t^{\min}_{i}, t^{\min}_{i+1}), \tag{13}$$

where $T^*_{\max}(i)$ is the time interval between the ith local maximum and the $(i-1)$th local maximum of $s(t)$. $T^*_{\min}(i)$ is the time interval between the ith local minimum and the $(i-1)$th local minimum of $s(t)$.

As defined, $\mu_1(\cdot)$, $\mu_2(\cdot)$ and $\mu_3(\cdot)$ are three measurements of the difference between the transmitter

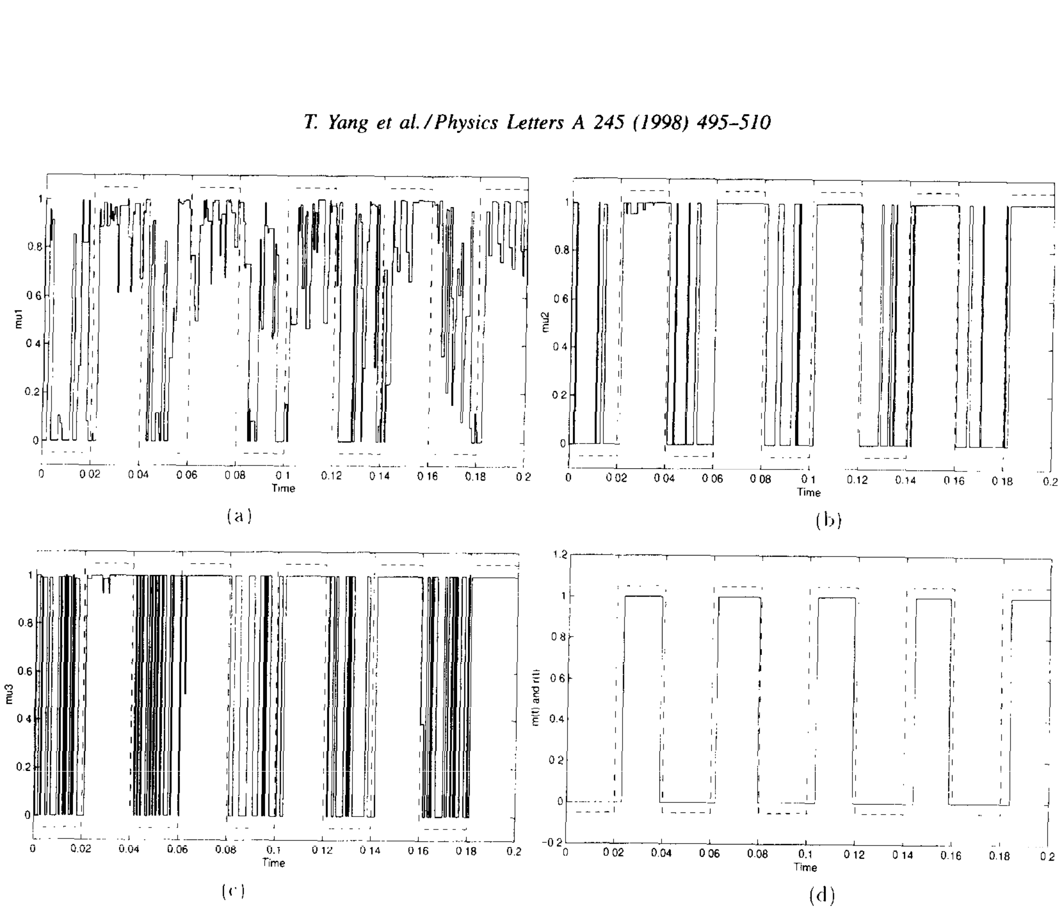


Fig. 3. Decoding chaotic shift keying. (a) $\mu_1(s(t))$ (solid line) and $m(t)$ (dash-dotted line). (b) $\mu_2(s(t))$ (solid line) and $m(t)$ (dash-dotted line). (c) $\mu_3(s(t))$ (solid line) and $m(t)$ (dash-dotted line). (d) The recovered signal $r(t)$ (solid line) and $m(t)$ (dash-dotted line).

and the standard transmitter. Since in chaotic shift keying, the parameters are switched between two sets, the changes of $\mu_1(\cdot)$, $\mu_2(\cdot)$ and $\mu_3(\cdot)$ can be used to detect this kind of switching even though we do not know in which attractor the transmitter is working. We use the following example to demonstrate this fact.

In this example the chaotic transmitter was switched between the standard parameter set and the second parameter set. Fig. 3a shows $\mu_1(s(t))$ with $\alpha = 0.04$. Since $\mu_1(s(t))$ denotes the degree of similarity between $s(t)$ and $v_1(t)$ of the standard transmitter, the big value of $\mu_1(s(t))$ denotes the high possibility of $m(t) = 1$. The peaks in the "0" phases correspond to the overlapped parts of the two return maps shown in Fig. 1a. The small membership values in the "1" phases occur because the observed values are outside the regions of two-second samples, which are used to construct the standard return map. At the end of the "1" phase and the beginning of the followed "0" phase, $\mu_1(s(t))$ keeps big for a while because there exists a transient process from the standard chaotic attractor to the second one. A similar process can be found during the switching process from phase "0" to phase "1".

Fig. 3b shows $\mu_2(s(t))$ with $\beta = 10^{-5}$. We can see that in the "1" phases the membership function keeps a big value all the time and in the "0" phases, it usually keeps small values except for some big impulses. From Fig. 1c we can see that there exist some overlaps in the first vertical line which has the biggest density of points. When the transmitter works in the "0" phases, there exist some chances that the points of the return map of the attractor in the "0" phase mix with the points in the first vertical line of the "1" phases. If this occurs, $\mu_2(s(t))$ gives high values even in the "0" phase.

Fig. 3c shows $\mu_3(s(t))$ with $\gamma = 10^{-5}$, which is similar to $\mu_2(s(t))$. From Figs. 3d and 3c, the message signal can be readily recovered by low-pass filtering and thresholding. Fig. 3d shows the recovered signal $r(t)$ (solid line) and the message signal $m(t)$.

Since the return map based method needs the peak information of the transmitted signal $s(t)$, if the switching frequency between two parameter sets is too high and comparable to the nature frequency of the attractor, then it is difficult to recover the message signal. However, the performance of chaotic shift keying may degrade dramatically if the switching frequency is too high. There should be a trade-off between the security and the performance of chaotic shift keying.

3.2. Security of chaotic parameter modulation

In Refs. [12,8], the authors proposed some chaotic parameter modulation schemes. In these schemes, message signals were used to modulate one or more parameters in the transmitters. At the receivers, message signals were recovered by using some adaptive control methods. The difference between chaotic shift keying and chaotic parameter modulation is that the former switching between two attractors and the latter gradually go through a set of attractors. The changes of the attractors become much smoother and more difficult to detect by return map based methods. However, we found that message signals can still be recovered with some distortions in phase and/or amplitude.

In the following example, we suppose that the standard return map is the same as that used in the previous subsection, and we use the following parameter modulation scheme:

$$C_1(t) = (17 + m(t))\ \mathrm{nF}, \tag{14}$$

$$L(t) = (12 + m(t))\ \mathrm{mH}, \tag{15}$$

$$m(t) = \sin(20\pi t). \tag{16}$$

This scheme is a softened version of the chaotic shift keying proposed in the previous subsection. Fig. 4a shows $\mu_1(s(t))$ with $\alpha = 0.005$. We can see that in this case the static value of $m(t)$ has no correspondence to the membership value. But when the message signal keeps small values, big membership values appear more frequently. When the message signal keeps big values, small membership values appear more frequently.

Fig. 4b shows $\mu_2(s(t))$ with $\beta = 10^{-6}$. We can see that the waveform is similar to pulse-width modulation of the message signal. When the message signal is smaller than a threshold, the output membership value always keeps 0.

Fig. 4c shows $\mu_3(s(t))$ with $\gamma = 10^{-5}$. We can see that in the vicinity of a negative peak of $m(t)$, the membership value becomes 0 for a long period. In the vicinity of a zero crossing of $m(t)$, the membership value will keep 1 for a short period.

Although from one of $\mu_1(s(t))$, $\mu_2(s(t))$ and $\mu_3(s(t))$ the message signal can not be easily detected, a combination of them can give more promising results. For example, in Fig. 4d, the combination of $\mu_2(s(t)) + \mu_3(s(t)) - 2\mu_1(s(t))$ and $m(t)$ are shown. One can see that $m(t)$ can be easily found from this combination by using a low-pass filter. The long-term evolution of the low-pass filtered result, $r(t)$, is shown in Fig. 4e. We can see that the basic structure of the message signal is recovered in $r(t)$. This is clearly shown in Fig. 4f, in which the power spectra of $m(t)$ and $r(t)$ are shown. We can see that the peak of the message signal clearly stands on the spectrum of $r(t)$.

4. Decoding non-autonomous chaotic modulation

In this section we call a transmitted signal *naked* if it is a state variable of the transmitter. We call a transmitted signal *compound* if it is a function of more than one state variable of the transmitter.

4.1. Naked transmitted signal

In Eq. (7), a non-autonomous chaotic modulation is presented. From Fig. 2 we can see that a big message signal can introduce significant differences in amplitude return maps. We can also see that $r^T_{\max}$ and $r^T_{\min}$ do not have enough horizontal changes for detecting the message signal. $r^A_{\min}$ has a bigger shift (as shown in Fig. 2b) than $r^A_{\max}$ (as shown in Fig. 2a). We also found that in this case, the shapes of the return maps are not changed, only shifts exist. To describe this kind of shift, we use the following measurement:

$$d(x,y) = -\min_{i=1}^{N-1}(V_{\min}(i) - x)^2 + (V_{\min}(i+1) - y)^2. \tag{17}$$

For comparison, $\mu_1(s(t))$ with $\alpha = 0.01$ is shown in Fig. 5a. $\mu_1(s(t))$ has a poor recovering quality as

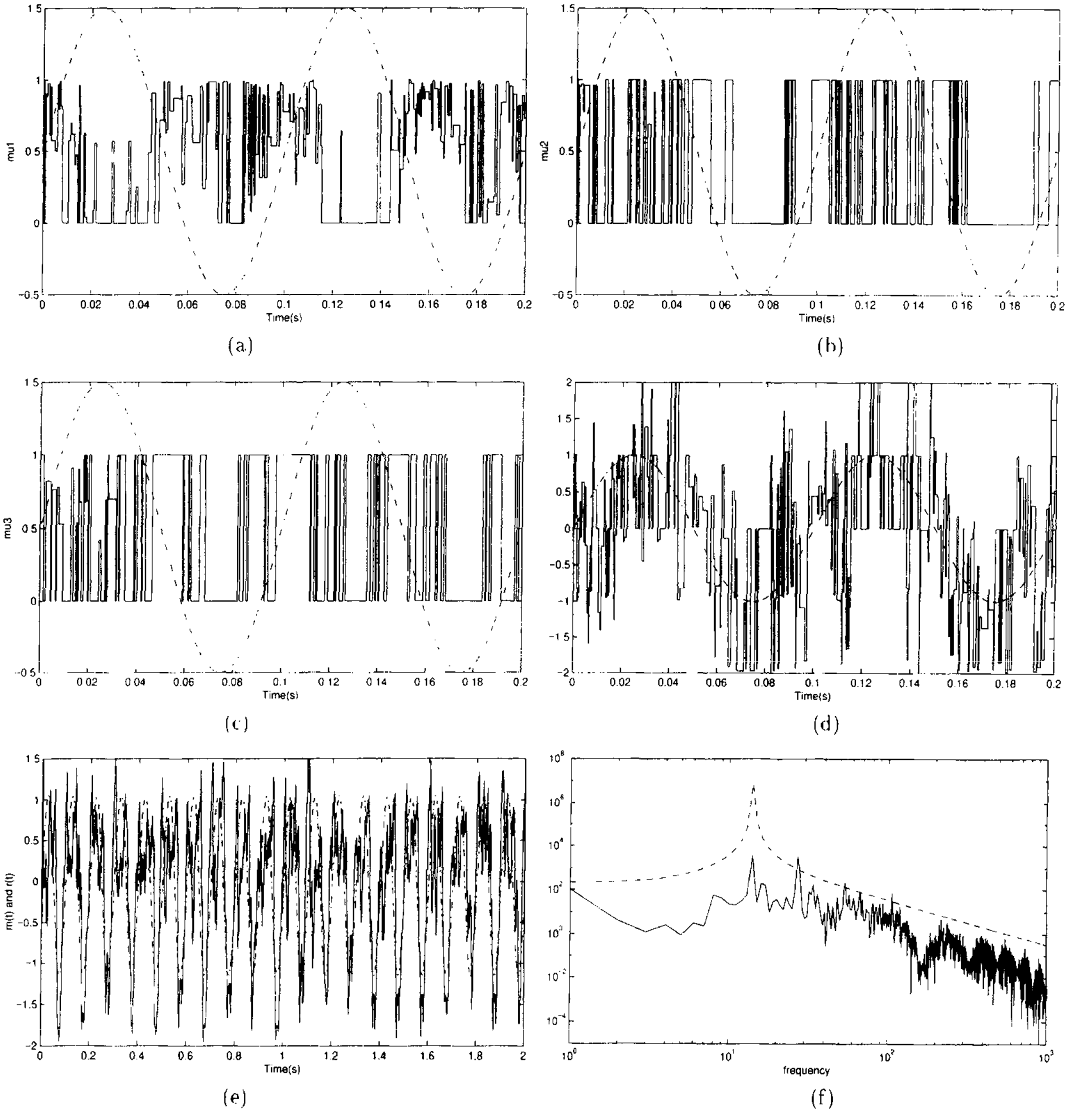


Fig. 4. Decoding chaotic parameter modulation with a sinusoidal message signal. (a) $\mu_1(s(t))$ (solid line) and $m(t)+0.5$ (dash-dotted line). (b) $\mu_2(s(t))$ (solid line) and $m(t)+0.5$ (dash-dotted line). (c) $\mu_3(s(t))$ (solid line) and $m(t)+0.5$ (dash-dotted line). (d) $\mu_2(s(t))+\mu_3(s(t))-2\mu_1(s(t))$ (solid line) and $m(t)$ (dash-dotted line). (e) The long-term evolution of the recovered signal $r(t)$ (solid line) and $m(t)$ (dash-dotted line). (f) The power spectrum of the recovered signal $r(t)$ (solid line) and that of the message signal $m(t)$ (dashed line).

shown in its low-pass filtered version, $r_1(t)$. We find $d(x,y)$ can provide a much better recovering quality, as shown in Fig. 5b. Observe that from $d(x,y)$ the message signal $m(t)$ can be easily recovered as shown in its low-pass filtered version $r_d(t)$. Fig. 5c shows the long-term evolution of $r_1(t)$. Although there exists big noise, the periodic structure of the message signal is clearly revealed. Fig. 5d shows the power spectra of $r_1(t)$ and $m(t)$. Observe that the peak of $m(t)$ clearly stands out from the power spectrum of $r_1(t)$. Fig. 5e shows the long-term evolution of $r_d(t)$. Comparing Figs. 5c and 5e we can see that $r_d(t)$ provides a higher signal-to-noise ratio (SNR). This can be verified by comparing Figs. 5d and 5f. We can see that the peak

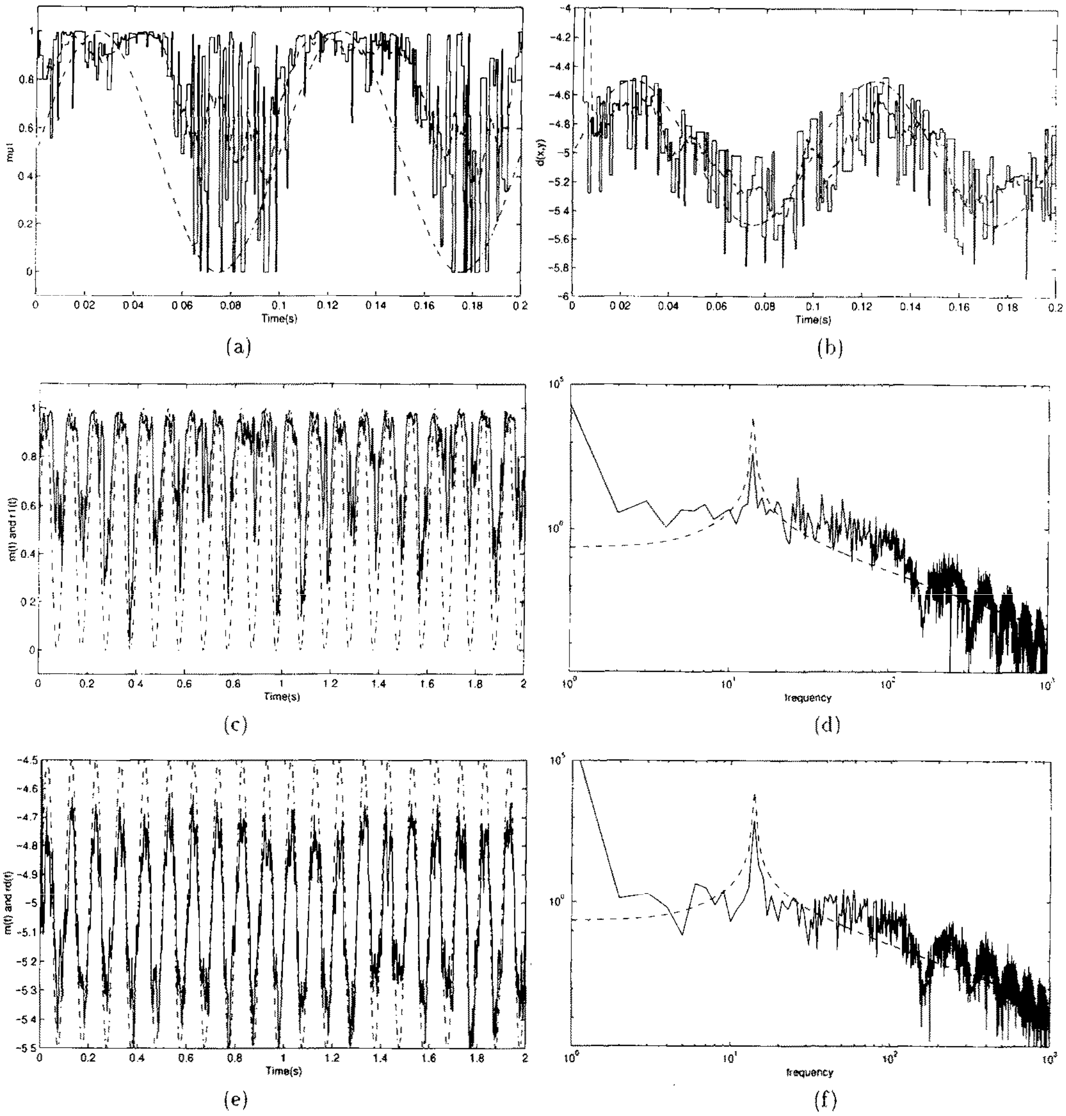


Fig. 5. Decoding non-autonomous chaotic modulation. (a) $\mu_1(s(t))$ (solid line), $50m(t)+0.5$ (dash-dotted line) and the low-pass filtered version of $\mu_1(s(t))$, $r_1(t)$ (dashed line). (b) $d(x,y)$ (solid line), $50m(t)-5$ (dash-dotted line) and the low-pass filtered version of $d(x,y)$, $r_d(t)$ (dashed line). (c) The long-term evolution of $r_1(t)$ (solid line) and $50m(t)+0.5$ (dash-dotted line). (d) The spectra of $r_1(t)$ (solid line) and $m(t)$ (dashed line). (e) The long-term evolution of $r_d(t)$ (solid line) and $50m(t)-5$ (dash-dotted line). (f) The spectra of $r_d(t)$ (solid line) and $m(t)$ (dashed line).

of the message signal in the power spectrum of $r_d(t)$ is higher than that in the power spectrum of $r_1(t)$. Comparing Figs. 4 and 5 we can see that the SNR of the recovered results of non-autonomous chaotic modulation is bigger than that of the chaotic parameter modulation.

4.2. Compound transmitted signal

In this scheme [15], more than one state variable of the chaotic transmitter is combined into a transmitted signal, $s(t)$. At the receiver end, the corresponding state variables are combined into a compound reference signal $\tilde{s}(t)$. While a feedback block makes the

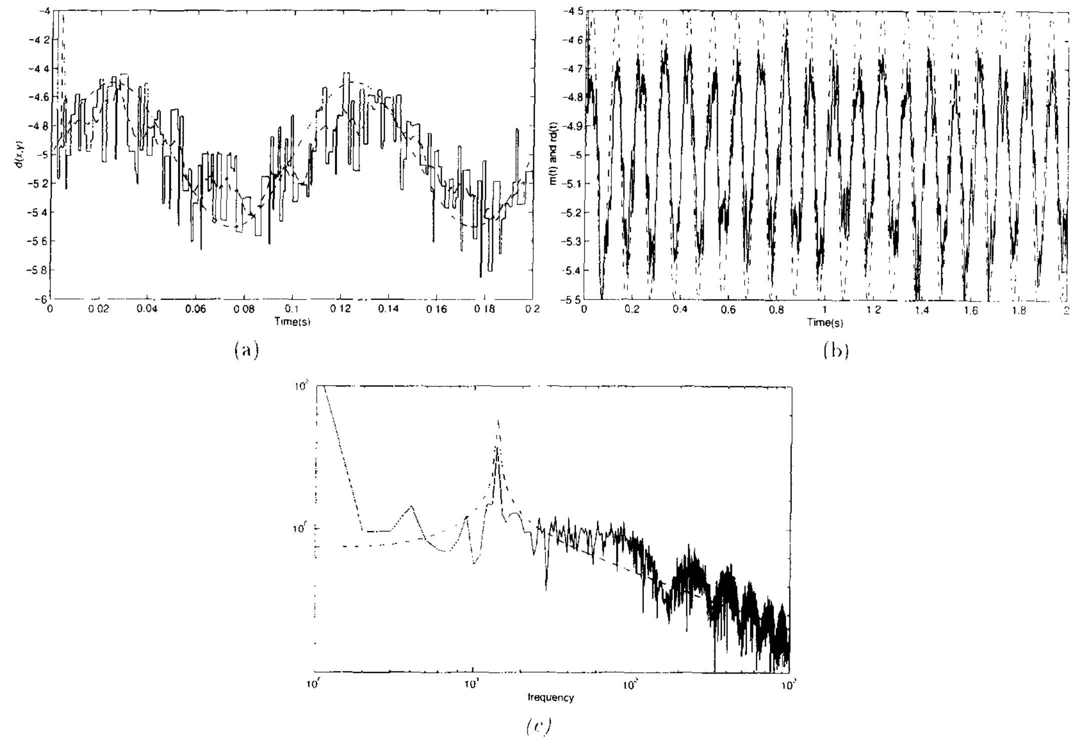


Fig. 6. Decoding compound transmitted signal method when $v_1(t) + v_2(t)$ is used as transmitted signal $s(t)$. (a) $d(x,y)$ (solid line), $50m(t) - 5$ (dash-dotted line) and the low-pass filtered version of $d(x,y)$, $r_d(t)$ (dashed line). (b) The long-term evolution of $r_d(t)$ (solid line) and $50m(t) - 5$ (dash-dotted line). (c) The spectra of $r_d(t)$ (solid line) and $m(t)$ (dashed line).

difference between $s(t)$ and $\bar{s}(t)$ zero, the synchronization between the transmitter and the receiver is achieved. Although in Ref. [15] the authors did not show how to apply this kind of chaotic synchronization to chaotic secure communications, their chaotic synchronization scheme can be easily used to transfer information. The authors of Ref. [15] also addressed that "the usage of a compound chaotic signal of more than one chaotic (state) variables to synchronize two chaotic systems can improve the security of a chaos-based secure communication system". Since it is not necessary for the compound signal to be more complex than its components, we should be careful to use this method. In this subsection, we study the security of the compound chaotic signal based methods.

Fig. 6 shows the decoding results using our methods. The compound transmitted signal is given by $s(t) = v_1(t) + v_2(t)$. To save space we do not give figures to show the changes of return maps. All the other conditions are the same as those in Subsection 4.1. Fig. 6a shows $d(x,y)$ and its low-pass filtered version, $r_d(t)$. For comparison, the message signal is also plotted. Fig. 6b shows the long-term evolution of $r_d(t)$. Fig. 6c shows the power spectra of $r_d(t)$ and $m(t)$. Observe that the peak of the message signal stands significantly out from the power spectrum of $r_d(t)$. Comparing Figs. 5f and 6c we can see that the compound signal method does not enhance the security significantly.

5. Performance under conditions of complicated return maps

Since the unmasking methods presented in this paper heavily depends on the structure of the return maps of the transmitted signal, a transmitted signal with complicated return maps should provide a high degree of security. In this section we show that this conjugation is true by using double-scroll attractors, which

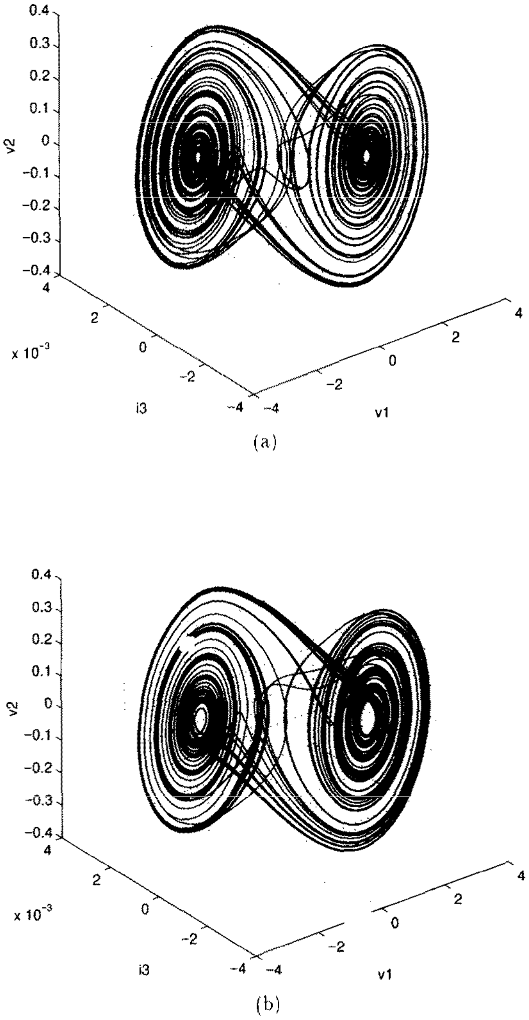


Fig. 7. The double-scroll chaotic attractors for the standard parameter set and the second parameter set. (a) The standard parameter set. (b) The second parameter set.

have more complicated return maps than Rössler-like attractors as studied in the previous sections.

The *standard parameters* for a Chua circuit to have a double-scroll attractor are given by: C_1 = 17 nF, C_2 = 178 nF, G = 1 mS, L = 12 mH, R_0 = 10 Ω, $G_a = -1.139$ mS, $G_b = -0.711$ mS, E = 1 V. In this section, the *second parameter set* is chosen as C_1 = 18 nF, C_2 = 178 nF, G = 1 mS, L = 13 mH, R_0 = 10 Ω, $G_a = -1.139$ mS, $G_b = -0.711$ mS, E = 1 V. We choose the differences between these two parameter sets to be the same as those in the previous sections. The chaotic attractors for the standard parameter set and the second parameter set are shown in Figs. 7a and 7b, respectively.

Similarly, if we choose $v_1(t)$ as the transmitted signal, the return maps for these two attractors are shown in Fig. 8[3]. Fig. 8a shows two $r^A_{\max}$ maps for two different parameter sets. Black points show the $r^A_{\max}$ map of Chua's circuit with the standard parameters. The grey points show the $r^A_{\max}$ map with the second parameter set. Although there exist some minor differences between both return maps, they are heavily mixed up. Fig. 8b shows two $r^A_{\min}$ maps. One can see that these two maps are also mixed up heavily. Fig. 8c shows $r^T_{\max}$. Observe that the return maps are much more complicated than that shown in Fig. 1c and the vertical shifts between these two maps are clearly visible. Fig. 8d shows $r^T_{\min}$. Also, the vertical shifts are clearly visible through there exists a heavy overlay in the vicinity of the first vertical curve. Comparing Fig. 8 with Fig. 1, we can see that the return maps in the former are much more complicated than those in the latter.

The results of unmasked chaotic parameter modulation when double-scroll attractors are used are shown in Fig. 9. Fig. 9a shows $\mu_1(s(t))$ with $\alpha = 0.001$; Fig. 9b shows $\mu_2(s(t))$ with $\alpha = 5\times10^{-5}$; Fig. 9c shows $\mu_3(s(t))$ with $\alpha = 10^{-5}$; Fig. 9d shows the combination of $\mu_2(s(t)) + \mu_3(s(t)) - 2\mu_1(s(t))$ and its low-pass filtered version $r(t)$. The long-term evolution of $r(t)$ is shown in Fig. 9e. Comparing with the results in Figs. 4e and 9e we can see that $m(t)$ should be much more difficult to find from Fig. 9e. Fig. 9f shows the power spectra of $r(t)$ and $m(t)$. Observe that in this case the peak of the message signal is still distinguishable.

6. Conclusions

In this paper, return map based chaotic cryptanalysis methods are proposed. In these methods, the cryptanal-

[3] Since the double-scroll attractor is symmetric with respect to the origin, we use $|v_1(t)|$ to construct the return maps. If we use $v_1(t)$ to construct return maps, then $r^A_{\max}$ (resp. $r^T_{\max}$) is symmetric to $r^A_{\min}$ (resp. $r^T_{\min}$) with respect to the origin.

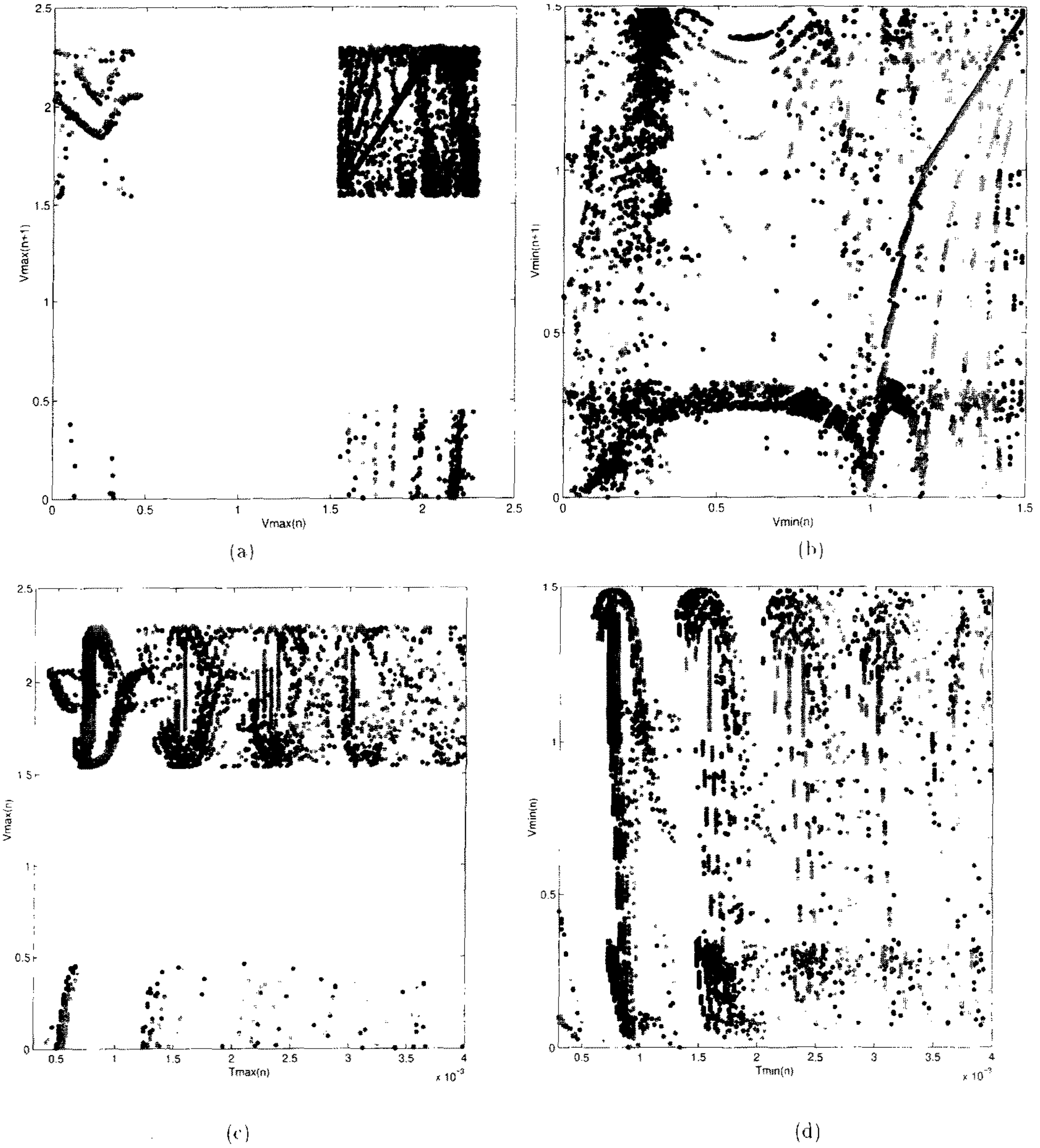


Fig. 8. The return maps of Chua's circuits with the standard parameter set and the second parameter set. Chua's circuits have double-scroll attractors. The black points show the return maps of the standard parameter set and the grey points show the return maps of the second parameter set. (a) $r^A_{\max}$, (b) $r^A_{\min}$, (c) $r^T_{\max}$, (d) $r^T_{\min}$.

ysis problems are translated into classification problems of return maps. Since many methods and tools are available to solve classification problems (e.g., fuzzy and neural network based methods), this transformation makes the chaotic cryptanalysis an easier task.

Since there exist many possibilities for constructing different kinds of return maps with respect to time and/or amplitude, the potential applications of return maps to chaotic cryptanalysis need further study. However, in this paper, by using four kinds of 2D return maps we can unmask chaotic shift keying, chaotic parameter modulation and non-autonomous

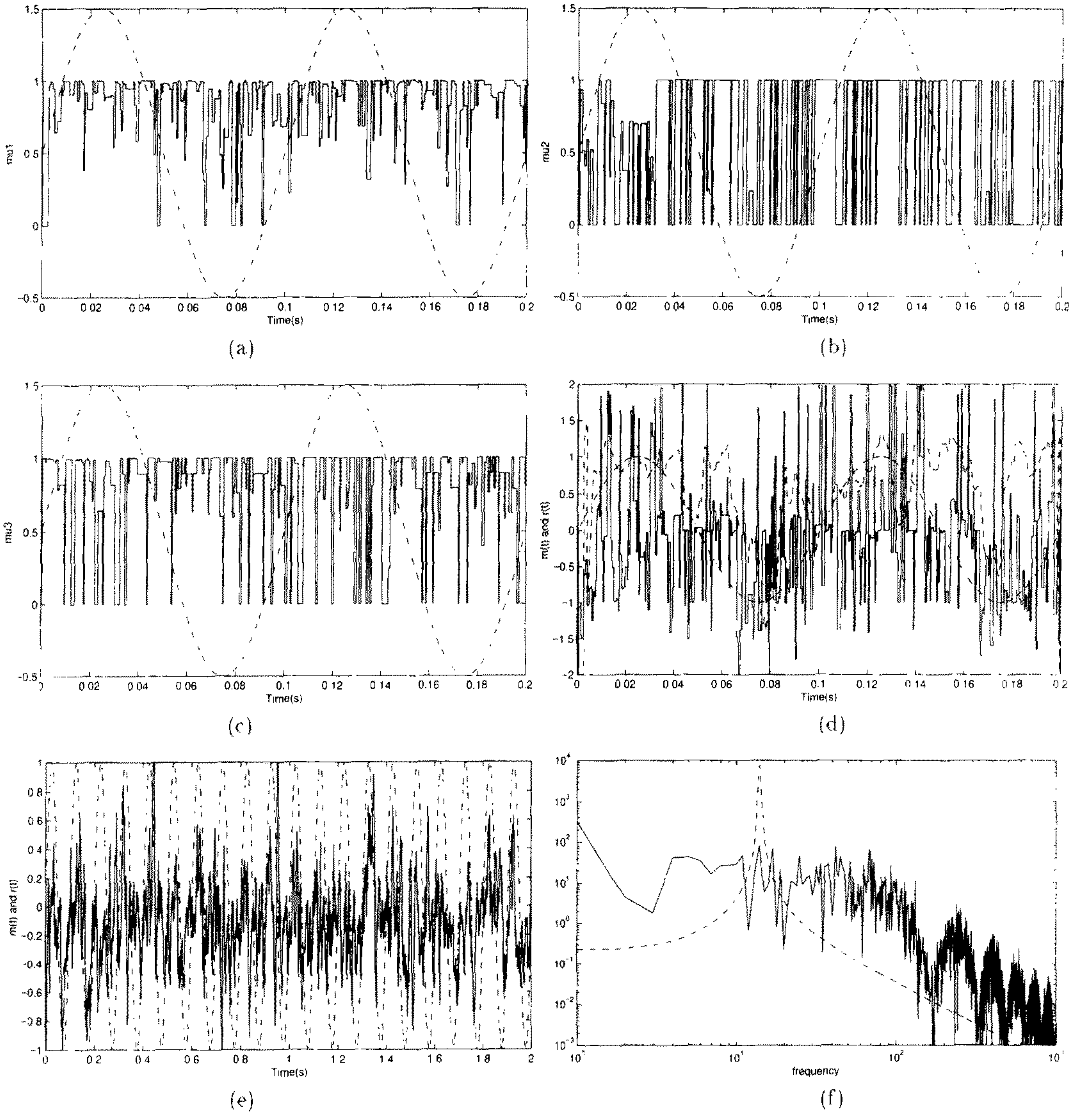


Fig. 9. Decoding chaotic parameter modulation with a sinusoidal message signal. The transmitter has double-scroll attractors. (a) $\mu_1(s(t))$ (solid line) and $m(t)+0.5$ (dash-dotted line). (b) $\mu_2(s(t))$ (solid line) and $m(t)+0.5$ (dash-dotted line). (c) $\mu_3(s(t))$ (solid line) and $m(t)+0.5$ (dash-dotted line). (d) $\mu_2(s(t))+\mu_3(s(t))-2\mu_1(s(t))$ (solid line) and $m(t)$ (dash-dotted line). (e) The long-term evolution of the recovered signal $r(t)$ (solid line) and $m(t)$ (dash-dotted line). (f) The power spectrum of the recovered signal $r(t)$ (solid line) and that of the message signal $m(t)$ (dashed line).

chaotic modulation easily. Our results show that the chaotic parameter modulation is more secure than non-autonomous chaotic modulation if the return map based attacks are used.

Although the message signals in our examples are very simple, our methods may be used in the cases when a more complex message signal, e.g., speech signal, is used. Since the human ear has an excellent adaptive ability, even the recovered speech signal is covered by big noise or even subject to some frequency band-shift, the *residual intelligibility*[4] in the recov-

[4] The residual intelligibility of a recovered signal is that propor-

ered message signal may be high enough for serious attacks [16].

Acknowledgement

This work is supported by the US Office of Naval Research under grant No. N00014-96-1-0753 and the Chinese Hong-Nian Yang Foundation under grant No. TLB01-1996.

References

[1] G.J. Simmons, Contemporary Cryptology: The Science of Information Integrity (IEEE, New York, 1992).
[2] K.M. Short, Int. J. Bifurcation Chaos 7 (1997) 1579.
[3] G.Pérez, H.A. Cerdeira, Phys. Rev. Lett. 74 (1995) 1970.
[4] K.M. Short, Int. J. Bifurcations Chaos 6 (1996) 367.
[5] K.M. Short, Int. J. Bifurcations Chaos 4 (1994) 957.
[6] T. Yang, Int. J. Circuit Theory Appl. 23 (1995) 611.
[7] T. Yang, L.B. Yang, C.M. Yang, Breaking chaotic switching using generalized synchronization: examples, IEEE Trans. Circuits Systems I (1998), in press.
[8] C.W. Wu, T. Yang, L.O. Chua, Int. J. Bifurcation Chaos 6 (1996) 455.
[9] T. Yang, C.W. Wu, L.O. Chua IEEE Trans. Circuits Systems I 44 (1997) 469.
[10] L.O. Chua, J. Circuit, Systems, Computers 4 (1994) 117.
[11] V. Parlitz, L.O. Chua, L. Kocarev, K.S. Halle, A. Shang, Int. J. Bifurcations Chaos 2 (1992) 973.
[12] T. Yang, L.O. Chua, IEEE Trans. on Circuits and Systems-I: Fundamental theory and applications 43 (1996).
[13] C.W. Wu, L.O. Chua, Int. J. Bifurcations Chaos 3 (1993) 1619.
[14] L. Zadeh, Info. Control 8 (1965) 338.
[15] K. Murali, M. Lakshmanan, Int. J. Bifurcations Chaos 7 (1997) 415.
[16] H.J. Beker, Analogue speech security systems, in: Cryptography Proc. of the Workshop on Cryptography, ed. T. Beth, Burg Feuerstein, Germany, 29 March–2 April 1982, pp. 130–146.

tion of the message signal which can be understood directly when listening to the recovered signal.