Time Scaling of Chaotic Systems: Application to Secure Communications

Donatello Materassi and Michele Basso

Dipartimento di Sistemi e Informatica, Università di Firenze

via S. Marta, 3, I-50139 Firenze (Italy)

(materassi@dsi.unifi.it / basso@dsi.unifi.it)

Abstract

The paper deals with time-scaling transformations of dynamical systems. Such scaling functions operate a change of coordinates on the time axis of the system trajectories preserving its phase portrait. Exploiting this property, a chaos encryption technique to transmit a binary signal through an analog channel is proposed. The scheme is based on a suitable time-scaling function which plays the role of a private key. The encoded transmitted signal is proved to resist known decryption attacks offering a secure and reliable communication.

Keywords: Chaotic Encryption, Secure Communication, Chaos Synchronization, Time-Scaling.

1 Introduction

In the last decades, encryption schemes that hide messages in chaotic signals have attracted attention as a tool to transmit information securely. The basic principle is to conceal the plaintext message using a chaotic signal and to recover it at the end of the receiver by means of a synchronization process [Pecora & Carrol, 1990]. In literature many techniques have been proposed, but they can be mainly divided into three different categories: Chaotic Masking, Chaotic Shifting Key and Chaotic Modulation.
Chaotic Masking has been the first encryption method introduced in chaotic communications. Basically, a chaotic signal (the "mask") is added to the plaintext to obtain the ciphertext. The synchronized receiver is able to recover the plaintext by simply subtracting the "mask" [Cuomo & Oppenheim, 1993].

In Chaotic Modulation a chaotic signal is modulated by the plaintext and the receiver recovers it through an "inversion" process that obviously depends on the modulation technique [Kolumban *et al.*, 1998].

In a wide sense, Chaotic Shifting Key (CSK) can also be seen as a special case of Chaotic Modulation. It allows the transmission of a binary signal by switching the parameters of two different chaotic systems. The receiver determines the bit value according to the success or failure of its synchronization attempt. Many cryptanalysis tools have been developed in order to evaluate the security of these schemes and it has been shown that the realization of secure communications based on chaotic encryption is still a quite difficult and challenging task [Li *et al.*, 2006].

In this paper we study classes of dynamical systems characterized by having the same phase diagram, but a different time response. This property reveals to be a useful countermeasure against known powerful decryption attacks (such as return map attacks). This suggests the possibility to effectively employ this kind of systems in chaotic communications. However, analysis of chaotic and, generally, nonlinear systems is quite complex to perform. This is the reason why an accurate cryptanalysis of communication schemes based on chaos encryption is difficult to realize and most employed tools are usually numerical simulations. Nevertheless, this work provides some theoretical results as a support to guarantee security of the system. The paper is organized as follows. In Section 2 the theoretical framework is described and developed; in Section 3 we propose a CSK scheme for secure communications exploiting time scaling functions; Section 4 is devoted to some qualitative cryptanalytical considerations and, finally, we provide some simulation results in Section 5.

2 Time Scaled Systems

Let us consider an autonomous dynamical system described by the differential equation

$$\frac{d}{dt}x = f(x) \qquad x \in \Re^n, f : \Re^n \to \Re^n. \tag{1}$$

We introduce a modified ("time-scaled") system

$$\frac{d}{dt}z = f(z)\lambda(z,t) \qquad z \in \Re^n, \lambda : (\Re^n \times \Re) \to \Re. \tag{2}$$

where λ is called "time scaling function". The effect of multiplying all the components of the function f by the same scalar function is just to modify the time scale of the original system [Sampei & Furuta, 1978]. The adoption of time scale functions is a quite common analysis tool in robotics and chemical applications because it gives some advantages in designing feedback linearizing controllers [Sampei & Furuta, 1978], [Respondek *et al.*, 2003] and, under some non-restrictive conditions, it does not change the stability properties of the system [Sampei

& Furuta, 1978]. However, in this work we are also interested into the fact that time scaling tranformations preserve most topological and geometrical properties of the phase diagram. For the sake of generality and completeness, we begin considering a time scale transformation depending both on time t and the state z. We report and prove some theoretical results which will be helpful for our purposes trying also to give an extensive overview.

Proposition 2.1 (Existence of the time scaled solution). *Let us consider systems (1) and (2). If there exists a solution $\phi_x(t, x_0)$ of (1) with initial condition $x(0) = x_0$ and if $\lambda(\cdot, \cdot)$ is "regular enough", then there exists a scalar function $\tau(t)$ such that $\phi_x(\tau(t), x_0)$ is a solution for (2) with the same initial value x_0.*

Proof. By hypothesis, the initial value problem

$$
\frac{dz}{d\tau} = f(z) \\
z(0) = x_0
$$

(3)

admits a solution $z(\tau) = \phi_x(\tau, x_0)$. Consider now

$$
\frac{d\tau}{dt} = \lambda(z(\tau), t) \\
\tau(t_0) = \tau_0.
$$

(4)

If $\lambda(z(\tau), t)$ is "regular enough", there exists a solution $\phi_\tau(t, t_0, \tau_0)$. Let $\tau(t) := \phi_\tau(t, 0, 0)$, we can define

$$
\phi_z(t, x_0) := \phi_x(\tau(t), x_0).
$$

(5)

By inspection, $\phi_z(t, x_0)$ is a trajectory of (2) with $t_0 = 0$ and $z(t_0) = x_0$. □

We remark that the "regularity" required on the time scale function λ is needed only to solve the Cauchy Problem (4). Actually, it could be sufficient to assume that λ is a piecewise locally Lipschitz function which definitely is not a restrective condition. However, if λ satisfies some additional properties, some more strict relations beetween the original and the "modified" system can be proved.

Proposition 2.2. *Under the conditions of Proposition 2.1 and assuming that $\exists\, l, L \in \Re$ such that $0 < l \leq \lambda(z, t) \leq L$, the phase diagrams of the two systems are identical.*

Proof. The proof is straightforward. Since $0 < l \leq \frac{d\tau}{dt} \leq L$, we can immediately conclude that $\tau(t)$ is continuous, increasing monotonic and therefore invertible on $\Re$. This means that every trajectory $\{\phi_x(t, x_0) | t \in \Re\}$ is completely mapped into the trajectory $\{\phi_z(t, x_0) | t \in \Re\}$. □

3

The previous proposition estabilishes a strong bond beetween the two systems. In fact, even though time responses can be very different, trajectories, attractors and stability properties of the two systems are exactly the same [Sampei & Furuta, 1978]. It is important to remark this holds for any kind of attractors, including strange attractors. Such a property will be exploited in the next section to derive a secure communication scheme.

Proposition 2.3. *Let v be a unitary vector in $\Re^n$. Define $y(t) = v^T x(t)$. Given two time instants $t_1 \leq t_2$, assume that $\{t \in [t_1, t_2] | \dot{y}(t) = 0\}$ is a discrete set. Consider also a time scale function*

$$\lambda(z) := \begin{cases} \Lambda_0 & \text{if } \lfloor v^T z/h \rfloor \text{ is even} \\ \Lambda_1 & \text{if } \lfloor v^T z/h \rfloor \text{ is odd} \end{cases} \tag{6}$$

where the symbol $\lfloor \cdot \rfloor$ denotes the floor function. Assume also that

$$2 \left(\frac{1}{\Lambda_0} + \frac{1}{\Lambda_1} \right)^{-1} = 1. \tag{7}$$

Then, under the conditions of Proposition 2.2

$$\lim_{h \to 0} \phi_z(t_2 - t_1, x_1) = \phi_x(t_2 - t_1, x_1). \tag{8}$$

Proof. The function λ "slices" $\Re^n$ by means of hyperplanes orthogonal to the vector v. In every "slice" (whose width is equal to h) the time scale is modified through a constant gain which is, alternatively, Λ_0 or Λ_1. Figure 1 schematically depicts this situation. With no loss of generality, we can assume $\Lambda_0 \leq \Lambda_1$. Since the harmonic mean (7) of the two values is one, we have $\Lambda_0 \leq 1 \leq \Lambda_1$. So, the time scaled system "moves" slower than the original one in those regions where $\lambda(z) = \Lambda_0$ and faster where $\lambda(z) = \Lambda_1$. However, if those regions are narrow enough (that means h "small" enough), the trajectory arc $x(\widehat{t_1)x}(t_2)$ is covered in the same amount of time by both the original and the scaled system. $\square$

3   Application to Chaos Encryption

In this section we will show how two time-scaled chaotic systems can be employed to send a binary signal in an encrypted manner. In particular, we will use two time-scaled chaotic systems in a chaotic shifting key (CSK) scheme showing how some security issues can be solved.

In a basic CSK scheme, the plaintext is encoded as a sequence of chaotic signals produced by one of two different chaotic systems according to the bit value. The receiver decodes the ciphertext through a simple on-off synchronization process. Consider the following system used as the sender
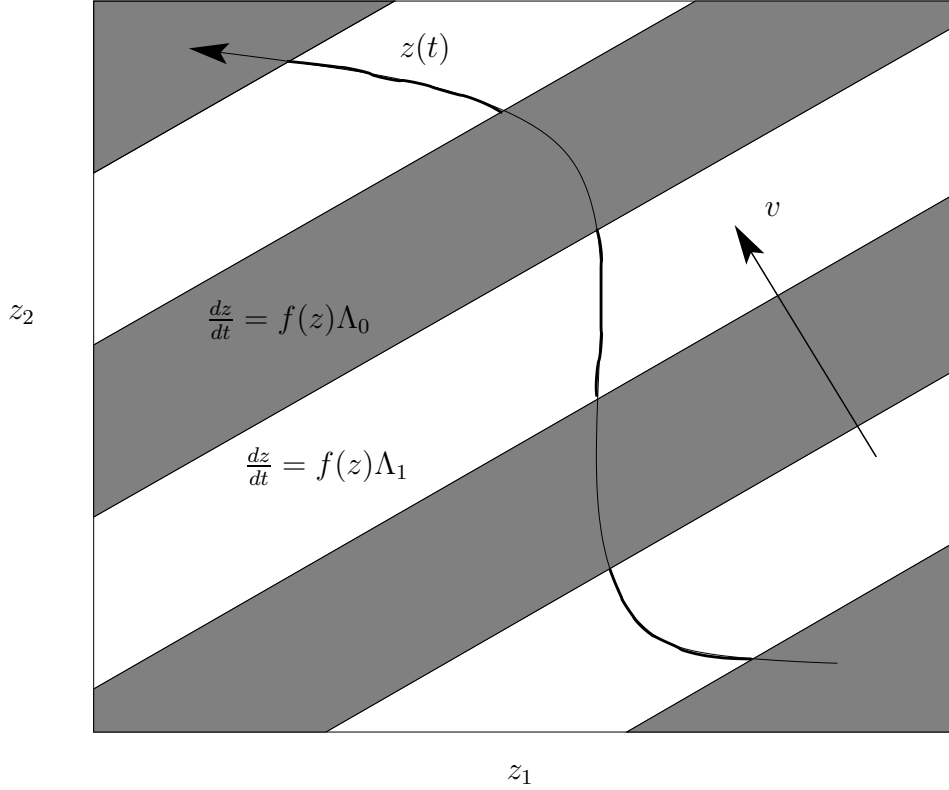
$$\dot{x} = f(x, s, \theta(m)) \tag{9}$$

4

Figure 1: Geometrical interpretation of Proposition 2.3.

where s is a scalar component of the state x and $\theta(m)$ is a vector of parameters modulated by a binary plain signal $m(t)$

$$\theta = \theta(m) = \begin{cases} \theta_0 & \text{if } m = 0 \\ \theta_1 & \text{if } m = 1. \end{cases} \tag{10}$$

Both θ_0 and θ_1 must have been suitably chosen to generate a chaotic regime in (9). To transmit $m(t)$, the signal $s(t)$ is sent out in order to cause synchronization to the receiver

$$\dot{z} = f(z, s, \theta_1). \tag{11}$$

If synchronization is achieved the bit is revealed to be 1, while, if there is no synchronization, the bit is concluded to be 0. The security of the system is based on the fact that an intruder would observe only the "apparently meaningless" chaotic signal $s(t)$ and should not be able to achieve synchronization without an accurate knowledge of the parameters θ_0 and θ_1 which play the role of a private key. Nevertheless, this basic scheme has been proved to be very vulnerable to Return Map attacks [Li *et al.*, 2006]. In fact, assuming that x_i and X_i are the $i-th$ minima and maxima, respectively, of s, we define the following variables $A_i := X_i + x_i$ and $B_i := X_i - x_i$. The plot of B_i as a function of A_i is called Return Map (RM) of the

5

signal s. The RM is topologically equivalent to the peak to peak dynamics plot described in [Candaten & Rinaldi, 2000]. An intruder, observing the encrypted signal $s(t)$, can easily reconstruct the RM with no knowledge of the parameters θ_0 or θ_1. In fact, if the two RMs of system (9) when $\theta = \theta_0$ and when $\theta = \theta_1$ are "well distinguishable", it is possible to unmask the concealed bit simply checking which map the transmitter is currently tuned on. An example of a RM reconstruction is reported in Figure 2. In this case the obtained RM shows two evident branches, one is associated to θ_0 and the other one to θ_1. The intruder, by simply checking what branch the transmitted signal is currently associated, can easily recover the plaintext sampled at every peak. Of course, the presence of channel noise would
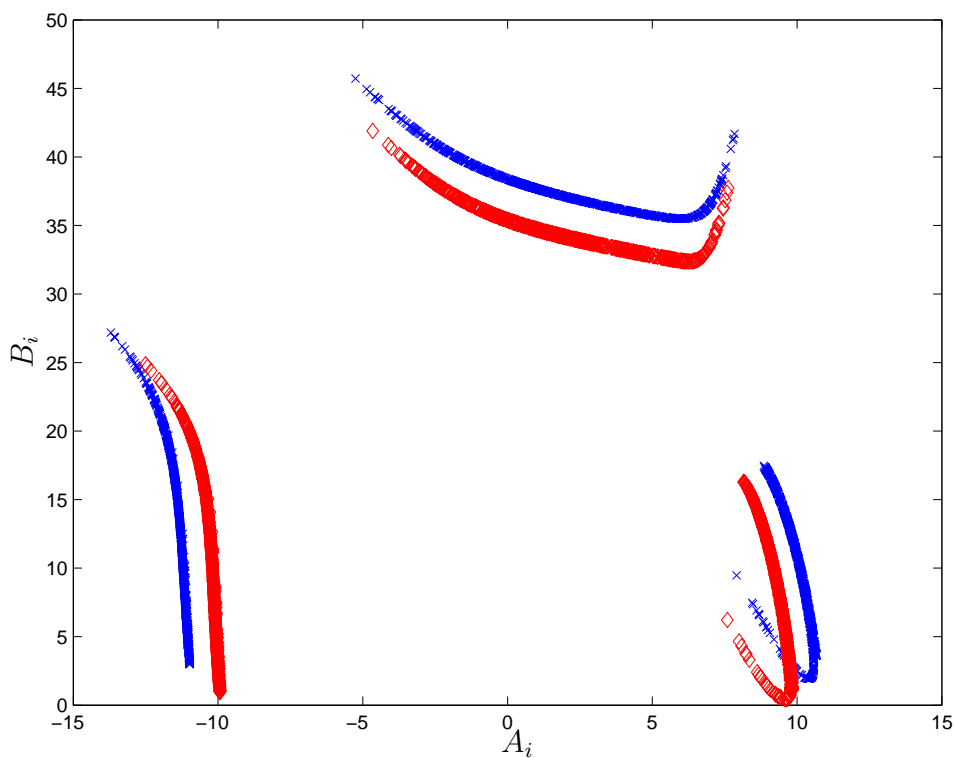

Figure 2: Two different values of the parameter θ in a CSK scheme can produce two distinguishable return maps.

disturb the attacker because he would obtain blurred maps. At the same time, we have to consider that noise would produce negative consequences on the receiver synchronization process, too. Many countermeasures have been considered in order to resist RM attacks (such as [Bu & Wang, 2004], [Palaniyandi & Lakshmanan, 2001]), and many of them have been broken, as well [Li *et al.*, 2006]. In [Xu & Chee, 2004] a very interesting approach has been proposed where the parameter θ still switches according to the plain-text bit value, but some more additional random switches are introduced to confuse a possible intruder. In this case,

the switching policy (10) is extended to the following form

$$\theta = \theta(x, m) \tag{12}$$

The additional pseudo-random switches occur according to one or more state variables (that are not transmitted), such that they do not disturb the receiver when it is in a synchronized condition. Conversely, this is novelty of the idea, an attacker trying to reconstruct the RM will be frustrated by the presence of many switches s/he is not able to predict because they are intrinsically related to the knowledge of the system structure. However, it is our opinion that the pseudo-random switch approach, in its general form described in [Xu & Chee, 2004], is still structurally vulnerable to RM attacks, if some precautions are not taken. Moreover, there are no theoretical results to guarantee that the reconstructed RM can not actually be exploited by an attacker.

3.1 Time Scale CSK scheme

The Time Scale CSK (TS-CSK) communication scheme we propose is partially inspired by [Xu & Chee, 2004], but it adopts time scaling functions to prevent the system to be broken by standard return map attacks. The transmitter and receiver have the following structure

$$\begin{aligned} \dot{x} &= f(x, s)\lambda(x, m) \\ \dot{z} &= f(z, s)\lambda(z, 1) \end{aligned} \tag{13}$$

where s is one of the state components which is being transmitted and $\lambda(x, m)$ is the strictly positive time scaling function

$$\lambda(x, m) = \left\{ \begin{array}{ll} \Lambda_m & \text{if } \lfloor v^T z/h \rfloor \text{ is even} \\ \Lambda_{1-m} & \text{if } \lfloor v^T z/h \rfloor \text{ is odd} \end{array} \right\} \tag{14}$$

such that Λ_0, Λ_1, v and h are fixed parameters chosen to meet condition of Proposition 2.3 which play .the role of the encryption key. In this case, the function λ defines a time-scale analogous to the time-scale described in Proposition 2.3 where the transmitted bit m simply inverts the roles of Λ_0 and Λ_1. This choice of λ is very demonstrative and it is motivated by its simplicity and by the theoretical results proved in the previous section. This peculiar structure allows to carry out some qualitative cryptanalytical considerations. Of course, a more sophisticated choice could bring to better results in terms of security, synchronization time and practical realization.

4 TS-CSK Cryptanalysis

In this section we will analyze how the proposed TS-CSK communication scheme can resist most common decryption attacks. This study does not intend to be an exhaustive cryptanal-

ysis since this can only be be accomplished describing the exact typology of attacks (known plaintext, known ciphertext, etc...). It is our aim to report only some qualitative considerations supported, when possible, by theoretical results.

4.1   Return Map attack

The communication system (13) is intrinsecally robust against a return map attack. In fact, from Proposition 2.2, it is obvious that, under practically non-restrictive conditions on f and λ, neither the modulation m nor the pseudo-random switches modify the phase portrait of the original non-timed scaled system

$$\dot{x} = f(x, s). \tag{15}$$

Therefore, the RMs of the TS-CSK scheme (13) and system (15) are exactly the same regardless of the transmitted bit $m(t)$.

4.2   Return Time Map attack

Assuming that X_i is the $i-th$ local maximum of $s(t)$ and t_i is the relative time instant when it occurs, we define the Return Time Map (RTM) as the plot of $t_{i+1} - t_i$ versus X_i. With no conceptual differences, the RTM could have been defined using the minima of $s(t)$ (or both minima and maxima) [Candaten & Rinaldi, 2000]. The effect of the function λ is to "speed up" the system when $\lambda > 1$ and to "slow down" it when $\lambda < 1$. It is intuitive that a wrong choice of the function λ could lead to a breakable system using a RTM attack [Candaten & Rinaldi, 2000].

By Proposition 2.3 it is immediate to conclude that if the number of time scaling switches is "dense" enough (with a proper choice of λ), then the RTM plot is not "significantly" modified by the time scaling. Of course, this is just a theoretical consideration, since the choice of a too small value for h would negate the possibility of a physical realization of such communication devices. However, Proposition 2.3 confirms the intuition suggesting small values for h in order to increase the security of the system.

4.3   Switch detection

In a CSK scheme, an intruder eavesdropping the communication could detect the changes of bit values by simply detecting discontinuities in the first derivative of the encoded signal $s(t)$. This is the reason why the adoption of a continuous function λ is deprecated. In fact, it would not create discontinuous false-switches analogous to the informative bit switches in order to confuse the intruder [Xu & Chee, 2004]. If false-switches are frequent enough in time and do

not depend on the drive signal it will be difficult to distinguish which ones will be informative. Again, the choice of small values for h seems to lead to increased security.

4.4 Brute Force attack

In a security analysis, it must be assumed that the intruder knows everything about the communication system structure, encryption method, physical characteristics (channel noise power spectrum etc...) but the encryption key. Nevertheless, the encryption key can be guessed, so it is important the key space is large enough in order to make such a guess the most difficult it is possible. A common problem in chaos communication is the fact that physical systems show a chaotic behaviour only in a very restricted range of their parameters limiting the choice of the key. The proposed approach, in its general form (13), overcomes this problem since there is no particular restriction on the function λ once it is assumed it is discontinuous and strictly positive.

5 Example

The communication system Pseudo Random Switch CSK (PRS-CSK) described in [Xu & Chee, 2004] exploits the well-known synchronization properties of two identical Lorenz models [Pecora & Carrol, 1990]

$$
\begin{aligned}
\dot{x}_1 &= \sigma(x_2 - x_1) \\
\dot{x}_2 &= (\beta - x_3)x_1 - x_2 \\
\dot{x}_3 &= x_1 x_2 - \rho x_3
\end{aligned}
\tag{16}
$$

$$
s = x_1
$$

$$
\begin{aligned}
\dot{z}_1 &= \sigma(z_2 - z_1) \\
\dot{z}_2 &= (\beta_0 - z_3)s - z_2 \\
\dot{z}_3 &= z_2 s - \rho z_3
\end{aligned}
$$

where $\theta(x, m) = [\sigma, \beta(m), \rho(x)]$. The parameter β is modulated the plain-text signal $m(t)$

$$
\beta(m) = \begin{cases} \beta_0 & \text{if } m = 0 \\ \beta_1 & \text{if } m = 1 \end{cases}
\tag{17}
$$

while the parameter ρ generates the false switching events

$$
\rho = \rho(x) = \begin{cases} b_1 & \text{if } a_1 < x_2 < a_2 \\ b_2 & \text{if } a_3 < x_2 < a_4 \\ b_3 & \text{if } a_5 < x_2 < a_6 \\ b_4 & \text{if } a_7 < x_2 < a_8 \\ b_5 & \text{otherwise} \end{cases}
\tag{18}
$$

In [Xu & Chee, 2004] the numerical choice of the variables was

$$
\begin{aligned}
\sigma &= 10 \\
\beta_0 &= 60.5 \\
\beta_1 &= 60 \\
a &= [0, 5, 31, 32, 23, 28, 10, 16] \\
b &= [10/3, 8/3, 2/3, 5/3, 2].
\end{aligned}
\tag{19}
$$

The transmission of 100 alternate bits (worst case scenario for the attacker) (as in [Xu & Chee, 2004]) has been simulated assuming the absence of channel noise using a standard ODE45 integration method with a relative tolerance of $1e - 12$ in order to obtain a low numerical noise. The result of the RM reconstructed by an eventual attacker is depicted in Figure 3. As
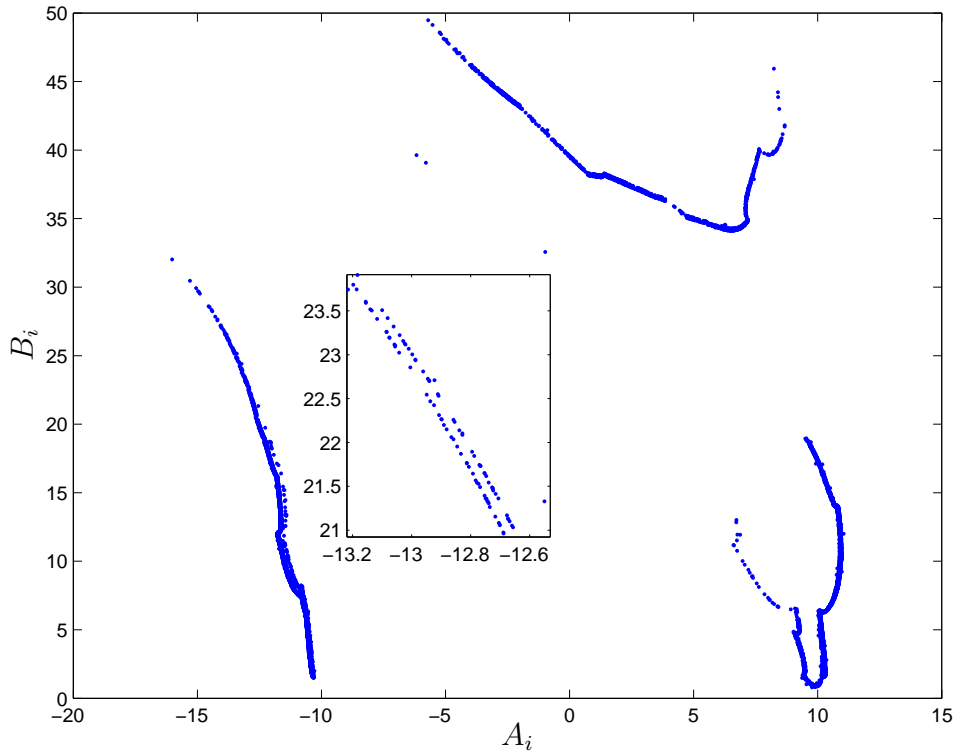
Figure 3: The Return Map of the PRS-CSK scheme (16), assuming no noise acting on che channel, still presents two distinct branches even adopting the pseudo-random switching CSK.

it is shown, in the RM two branches are still distinguishible even though they are definetely close. However, the close distance of the two branches is mainly related to the fact that the two values β_0 and β_1 are pretty similar. In a practical situation, the two branches would be very likely undistinguishable because of channel noise, but, as we have previously stressed, the

presence of noise may disturb the receiver synchronization as well. A theoretical guarantee that a RM attack is really ineffective would be desirable from the security point of view.

As a comparison, we employ the same Lorenz model in a TS-CSK communication scheme

$$\dot{x}_1 = [\sigma(x_2 - x_1)]\lambda(x, m)$$
$$\dot{x}_2 = [(\beta - x_3)x_1 - x_2]\lambda(x, m)$$
$$\dot{x}_3 = [x_1 x_2 - \rho x_3]\lambda(x, m)$$

$$s = x_1 \tag{20}$$

$$\dot{z}_1 = [\sigma(z_2 - z_1)]\lambda(z, 1)$$
$$\dot{z}_2 = [(\beta - z_3)s - z_2]\lambda(z, 1)$$
$$\dot{z}_3 = [z_2 s - \rho z_3]\lambda(z, 1)$$

with $\sigma = 10$, $\beta = 60$, $\rho = 2$ and using $\lambda(x, m)$ in (14) with the private encryption/decryption key

$$v = [0, 1, 0]^T$$
$$h = 2$$
$$\Lambda_0 = 15/16$$
$$\Lambda_1 = 15/14.$$

Figure 4 shows the Lorenz attractor projected on the plane x_1-x_2 along with the time-scale policy. Given the bit m to be transmitted, in the white stripes the system evolves with the time-scale factor Λ_m while in the gray ones the time-scale factor Λ_{1-m} is used. System (20) has been simulated with the transmission of 100 alternate bits (ODE45 solver with relative precision equal to $1e-12$). The corresponding RM and RTM obtained by an eventual intruder are reported in Figures 5 and 6, respectively. Return Map Attack is completely countered since the RM of the the sender dynamics does not change according to the bit value. Moreover, a RTM based attack does not seem to be so effective because the map is sparse enough not to reveal the presence of distinct branches (we are implicitly assuming that the integration error in the simulation procedure can be safely neglected). In order to show that the proposed scheme can provide a secure and reliable communication, Figure 7 depicts the simulation results of the decryption phase at the receiver. Ten alternate bits have been encoded and the right synchronizations/desynchronizations occur very promptly.

6 Conclusion

An encryption scheme to send digital data through an analog channel has been introduced by exploiting a class of time scaling functions. It has been proved that such a scheme is
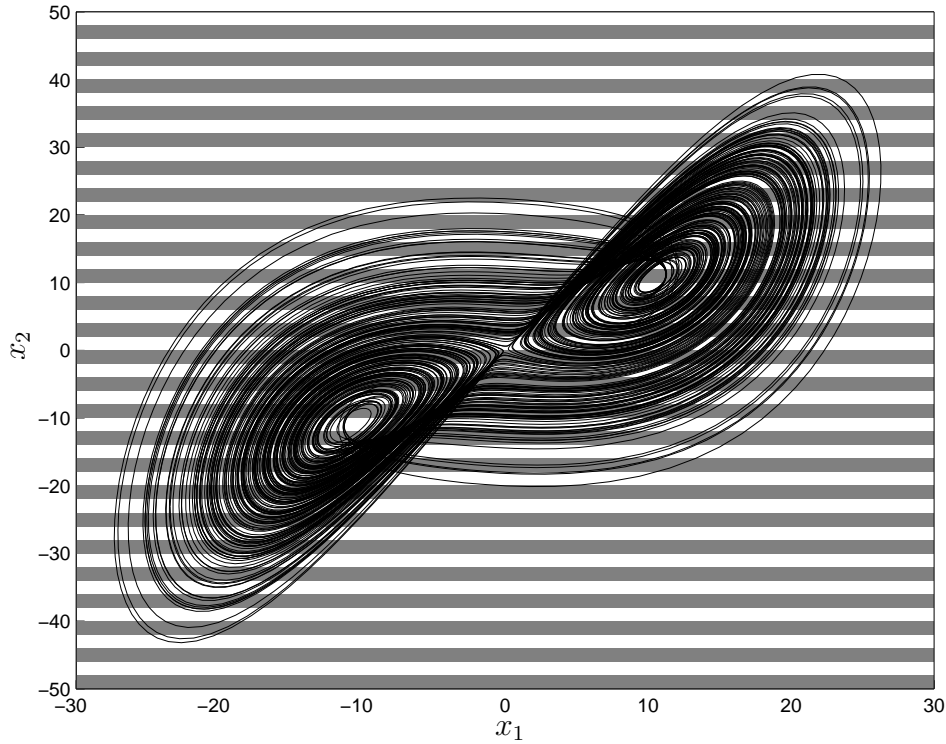
Figure 4: Projection of the Lorenz attractor on the plane x_1-x_2 for the TS-CSK scheme.

intrinsecally secure against simple return map attacks. Some theoretical results show that return time map attacks should not be so effective, too, if the choice of the time-scaling function satisfies some requirements. Switch detection beetween bits in the plaintext is also made difficult by using a pseudo-random false-switching technique. Simulations show effectiveness of the proposed communication scheme with respect to known decryption attacks.

References

Bu, S. & Wang, B. H. [2004] "Improving the security of chaotic encryption by using a simple modulating method," *Chaos Solitons and Fractals* **19**(4), 919–924.

Candaten, M. & Rinaldi, S. [2000] "Peak to peak dynamics: a critical survey," *International Journal of Bifurcation and Chaos* **10**(8), 1805–1819.

Cuomo, K. M. & Oppenheim, A. V. [1993] "Chaotic signals and systems for communications," in *Proc. of International Conference on Acoustics, Speech, and Signal Processing* (Minneapolis (MN)).
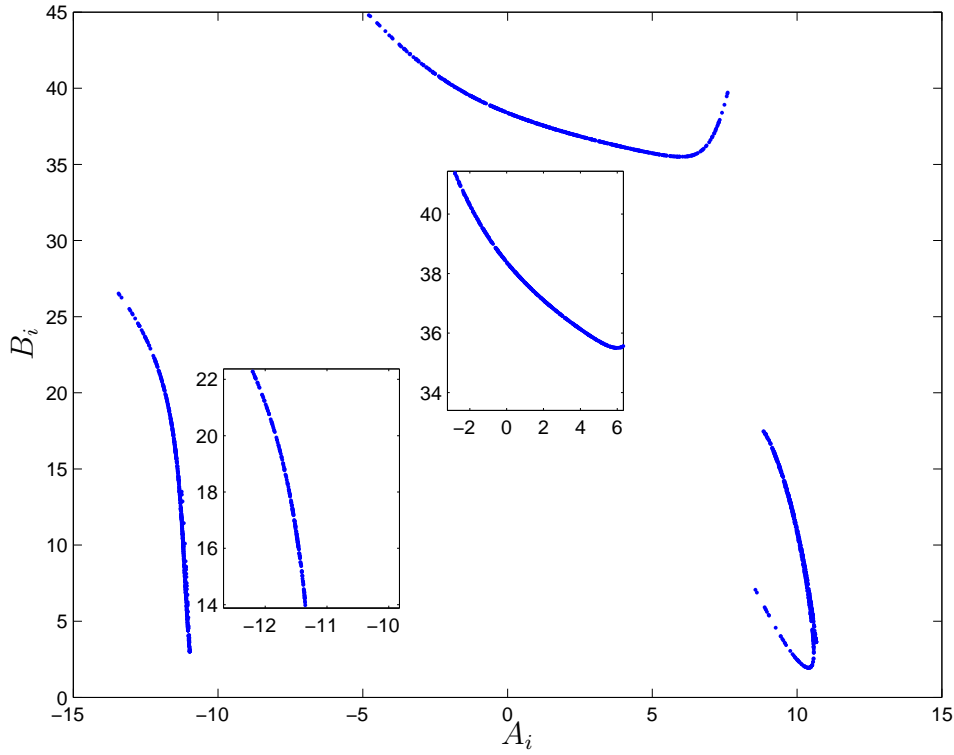
Figure 5: TS-CSK: Return Map attack is completely countered since the RM of the the sender dynamics in (20) does not change according to the bit value.

Kolumban, G., Kennedy, M. & Chua, L. O. [1998] "The role of synchronization in digital communications using chaos. Part II. chaotic modulation and chaotic synchronization," *Circuits and Systems I: Fundamental Theory and Applications* **45**(11), 1129–1140.

Li, S., Chen, G. & Alvarez, G. [2006] "Return-map cryptanalysis revisited," *International Journal of Bifurcation and Chaos* **16**(5), 1557–1168.

Palaniyandi, P. & Lakshmanan, M. [2001] "Secure digital signal transmission by multistep parameter modulation and alternative driving of transmitter variables," *International Journal of Bifurcation and Chaos* **11**(7), 2031–2036.

Pecora, L. M. & Carrol, T. L. [1990] "Synchronization in chaotic systems analysis and design," *Physical Review Letters* **64**, 821–824.

Respondek, W., Pogromsky, A. & Nijmeijer, H. [2003] "On time scaling for nonlinear systems: Application to linearization," *Automatica* **40**(2), 277–285.

Sampei, M. & Furuta, K. [1978] "On time scaling for nonlinear systems: Application to linearization," *IEEE Transactions on Automatic Control* **31**(5), 459–462.
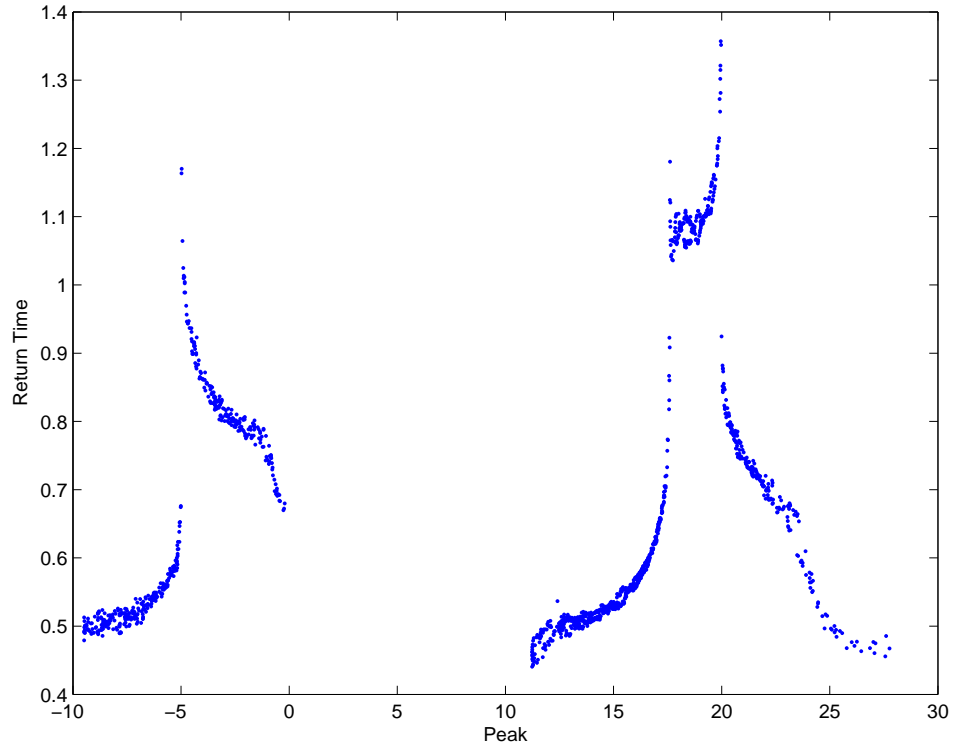
Figure 6: TS-CSK: Return Time attack originates a sparse map which makes it difficult to crack the system.

Xu, D. & Chee, C. Y. [2004] "Chaotic encryption with transient dynamics induced by pseudo-random switching keys," *International Journal of Bifurcation and Chaos* **14**(10), 3625–3631.
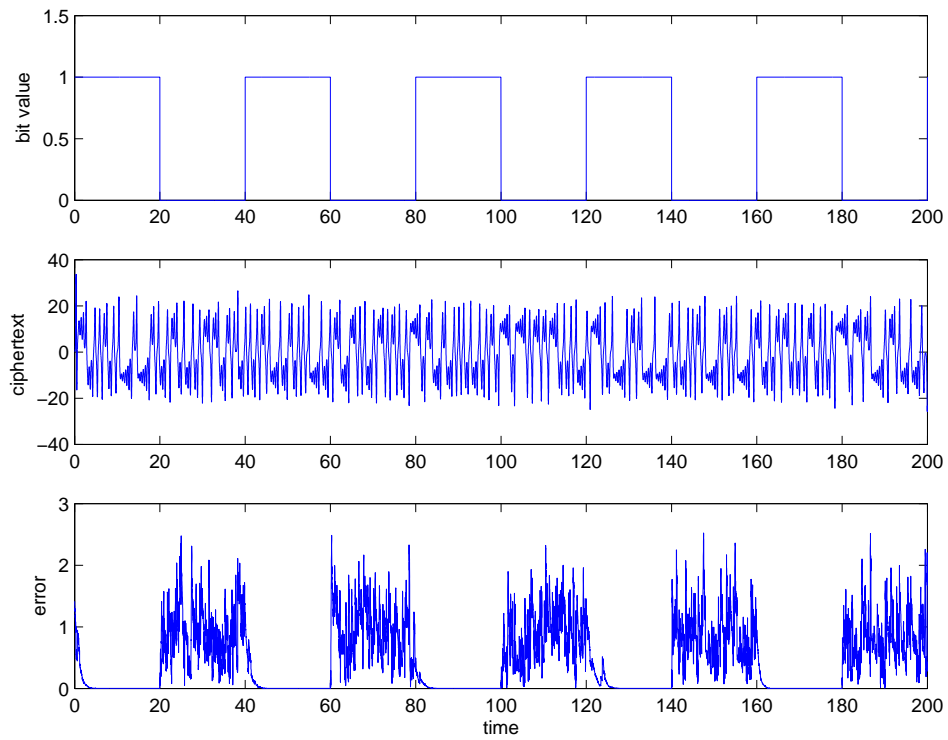
Figure 7: TS-CSK: Transmission of ten alternate bits, the ciphertext and the relative synchronization error at the receiver end.