Application of observer-based chaotic synchronization and identifiability to original CSK model for secure information transmission

Oleg Garasym, Ina Taralova, René Lozi

Application of observer-based chaotic synchronization and identifiability to original CSK model for secure information transmission

Oleg Garasym
IRCCyN UMR CNRS 6597, Ecole Centrale de Nantes
Nantes, France, 44300
Oleg.garasym@irccyn.ec-nantes.fr

Ina Taralova
IRCCyN UMR CNRS 6597, Ecole Centrale de Nantes
Nantes, France, 44300
Ina.taralova@irccyn.ec-nantes.fr

René Lozi
Université de Nice Sophia-Antipolis, Laboratoire J. A. Dieudonné, UMR CNRS 7351, Parc Valrose
Nice, France, 06102
rlozi@unice.fr

Received (to be inserted by publisher)

Modified Lozi system is analyzed as chaotic PRNG and synchronized via observers. The objective of the study is to investigate chaotic-based encryption method that preserves CSK model advantages, but improves the security level. CSK model have been discussed to message encryption because it implies better resistance against noise, but there are many evidences of the model weaknesses. The investigation provides the original CSK model analyses of secure message transmission over the communication channel by examining identifiability and observability; switched regimes detection; sensitivity to initial conditions and session key; NIST tests of the encrypted signal; correlation between wrong decrypted messages; system ergodicity. The proposed model has a significant effect on the security level of the transmitted signal that successfully passed chaotic and randomness tests. The results suggest that the original CSK model can be used for information security applications.

Keywords: generator, security, encryption, switched chaotic model, generators shifting.

1. INTRODUCTION

Cryptographic protection is one of the information systems security directions that is used in ATMs, digital television, Internet-payments etc. The cryptographic methods of information security could be realized by both ways: software or hardware. Software implementation of encryption is cheaper and practical. In almost all cases, software encryption is based on pseudo random number generators (PRNG). Consequently, PRNG must have excellent randomness properties and to be robust against attacks. In addition, the original information (data, message) is mixed up with the PRNG dynamics that are challenging for the chaos-based cryptosystem implementation. In the case of chaotic PRNG, essential cryptogram modifications of the same text appear while the initial conditions (starting points) are even slightly incorrect. Chaotic

generators application is a challenging task to the secure information transmission. The chaotic application is represented in different models [Hasan M. & Idris I., 2012; Liu, J. & Zhang, Y. , 2011] that are based on chaotic synchronization to decrypt the "information" (digital text information, pin codes, images etc.) on the receiver part. Due to chaotic reactiveness to the initial condition, synchronization is required to be precisely performed otherwise synchronization error increases with every next step, which leads to incorrect message recovery. Thus, several models like [Terry, J. & VanWiggeren, G. , 2001] have been proposed to use additional communication channel but making difficult real-life implementation. In addition there are other requirements for cryptosystems such as: confidentiality (saving secrecy), integrity (changes should be made only by permission of the object and to use the allowed mechanisms), availability (information is useless if it is not available), speed performance, robustness against noise etc. One of the most difficult tasks on the key-stream chaotic cryptosystem way is observer design. The role of the observer is to guarantee the system state recovery of the transmitter from the output signal. If the states are restored, the signal could be synchronized (obtaining the same dynamics) on the receiver part as on the transmitter part. Synchronization is applied to recover the message on the receiver part of a secure system. Successful synchronization performing is determined by high accuracy because of chaos sensitivity.

The papers [Liang, X. & Zhang, J. & Xia, X. , 2008; Anstett, F. & Millerioux, G. & Bloch, G. , 2006] prove that identifiable parameters of the chaotic system are not suitable for secure message transmission. The papers demonstrate techniques on possibilities to refund secret parameters from the output signal. However, there are some cases where identifiable parameters are required [Dedieu, H. & Ogorzalek, M. , 1995; Anstett, F. & Millerioux, G. & Bloch, G. , 2006]. The papers explain moments when non-identifiable parameters simplifies attacks fulfilling to the system. It is demonstrated that non-identifiable parameters reduce the set of possible secret key simplifying for adversary brute-force attack. Nevertheless, from control theory point of view, synchronization is achieved via observer design: the chaotic generator has to be observable and its parameters to be known (identifiable).

For the first time, the parameters of the Lozi system are analysed on observability and identifiability. The synchronization results are used for the message decryption in an original model. The original model with generators shifting ensures the secure message transmission either the system is identifiable or non-identifiable.

The paper is organized as follows: after a problem statement (section 2), we deal with the system identifiability analysis (section 3) and synchronization via observers design (section 4). Then we propose an original chaos encryption scheme based on z-shifting chaotic generators (section 5) and apply required criteria to prove the excellent statistical system properties (section 6) compared of the original one (section 7).

2. PROBLEM STATEMENT

From control theory point of view to perform signal synchronization between transmitter and receiver, the system has to be observable. The system parameters are used as a secret key, precise knowledge of which is required. From the information security point of view the system has to be verified for identifiability [Anstett, F. & Millerioux, G. & Bloch, G. , 2006; Dedieu, H. & Ogorzalek, M. , 1997; Xia, X. & Moog, C. , 2003] to avoid weakness when the secret key can be recovered from the output signal.

The chaotic dynamics is easily influenced by any changes. Consequently, noise in the communication channel is the challenging issue to achieve synchronization. Chaotic shift keying or switching model (CSK) is considered by numerous authors [Hasler & Martin, 1998; Uchida, A. & Yoshimori, S. , 2001; Heil, T. & Mulet, J. , 2002] due to its better resistance to noise than others models [Hasan M. & Idris I., 2012; Yang, T. , 2004]. The general model is based on two chaotic generators that are used to encrypt binary message. The first generator encrypts the bit "1" and the second bit "0". The switch-modulated method is proposed in [Wang, X. & Gao, Y. , 2010] based on switching regimes where each of the generators corresponds for encryption by pair-bits. The multiple chaotic generators application from one hand increases signal complexity [Xiao, Y. & Han, Y. , 2007], on the other hand, makes chaotic synchronization perform too slow and fragile in the presence of noise. Thus, the mentioned model is not robust.

In the interest of confidentiality, it is preferable that the generators in CSK model start from different

initial conditions, but the qualitative features have to be identical. The difference in generators dynamics leads to the possibility to detect message without knowing chaos generator structure and initial conditions [Yang, T. & Yang, L. & Yang, C. , 1998]. Let us consider an example with 2 generators: the first one is chaotic which is applied to encrypt the bit "1"; the second is sine wave which encrypts the bit "0" (Fig.1). Bernoulli binary block is used to simulate a binary message because of its good statistical and distribution properties. The approach is highly insecure due to the difference in generators dynamics. The message is recognizable without any additional methods only by looking on the signal (Fig.2). It is possible to determine when switching was performed, therefore, to detect bits of the message. No doubt, the switching regime detection between 2 chaotic generators is the challenging task. However, the approach of breaking CSK model with two chaotic generators is given in the paper [Yang, T. & Yang, L. & Yang, C. , 1998]. The method uses spectrogram and filters for the differences detection in the signal that are corresponding to the message bits. The paper proved it week security that is an additional evidence of the CSK model insecurity.

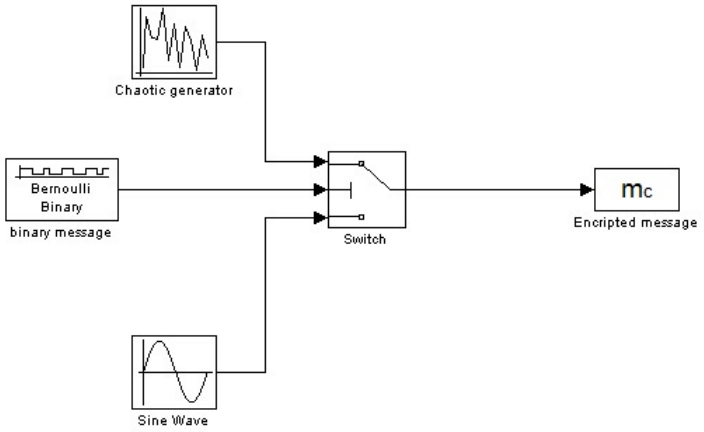


Fig. 1. Chaotic generator and sine wave application for message encryption in the CSK model

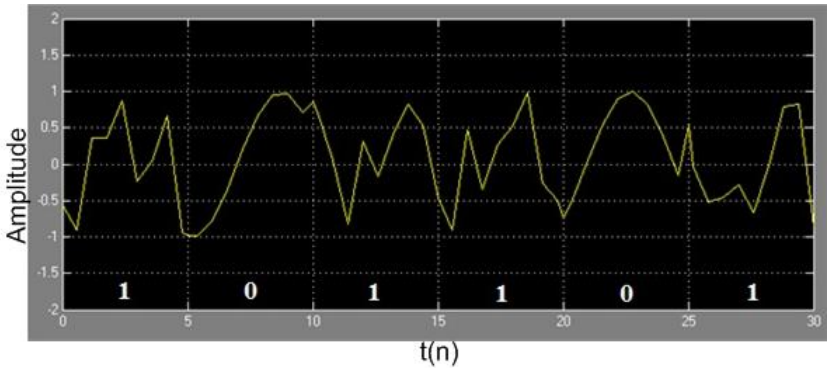


Fig. 2. Decryption message from the signal

The encrypted message m_c (Fig.1) by chaotic generator and sine wave can be visually recovered because of their different dynamics (Fig. 2). To avoid such kind of risk the switched chaotic generators must have qualitatively identical statistical and spectral properties.

The new Lozi alternate system with auto-coupling and ring-coupling [Lozi, R. , 2012] has been selected because it satisfies the above conditions. Moreover, the system has good randomness and high chaoticity

[Garasym O. & Taralova I. , 2013]. It has passed successfully statistical and numerical tests such as: auto-correlation; cross-correlation; uniform distribution; chaoticity where $x \in R^p$, $T^p = [-1,1]^p$ by the map $M_p = T^p \to T^p$:

$$M_p : \begin{cases} x^1_{n+1} = 1 - 2|x^1_n| + k^1((1-e_1)x^2_n + e_1 x^1_n) \\ x^2_{n+1} = 1 - 2|x^2_n| + k^2((1-e_2)x^3_n + e_2 x^2_n) \\ \vdots \\ x^p_{n+1} = 1 - 2|x^p_n| + k^2((1-e_p)x^1_n + e_p x^p_n) \end{cases} \tag{1}$$

$$y_n = C x^1_n$$

Where the parameters $k^j = (-1)^{j+1}$, $e_p \in]0,1[$ and y_n is the output signal used for the message encryption. The output equals only to one of the system states. The graph of the map $-2|x^p_n|$ is the tent map. It should be pointed that the map M_p is normally diverging. To avoid divergence (Fig. 3) the following injection mechanizm has to be fulfilled that trajectories are fed back to the torus $[-1,1]^p$:

$$\begin{array}{c} \text{if } x^j_{n+1} < -1 \text{ then add } 2 \\ \text{if } x^j_{n+1} > 1 \text{ then substract } 2 \end{array} \tag{2}$$

The injection mechanism (2) allows to keep the system dynamics in the interval $[-1,1]$ and makes it more complex.

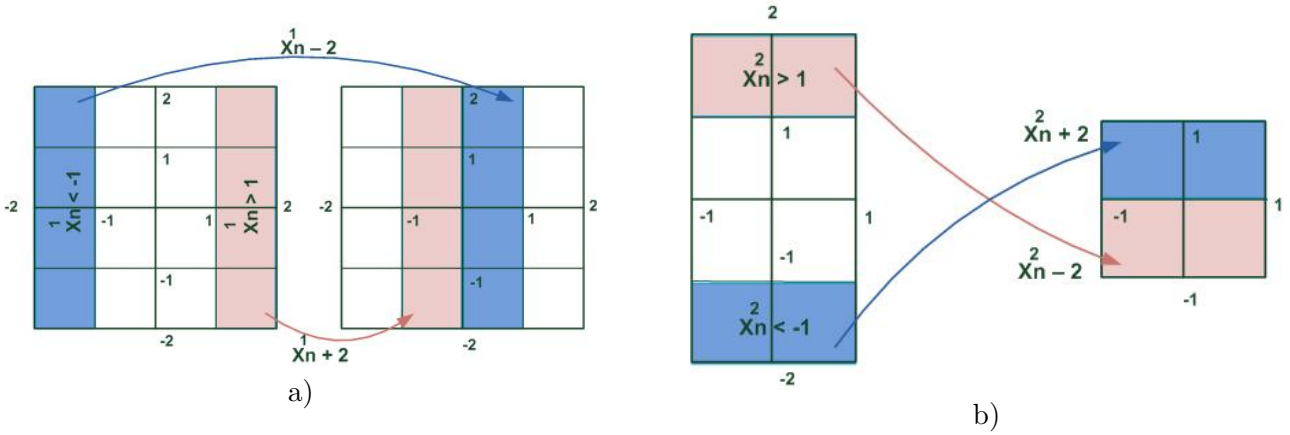


Fig. 3. Injection mechanism of the trajectories back to the torus ($[-2,2]^2 \Rightarrow [-1,1]^2$) **a)** if $x^{(1)}_n > 1$ then $x^{(1)}_n - 2$ or if $x^{(1)}_n < -1$ then $x^{(1)}_n + 2$ **b)** if $x^{(2)}_n > 1$ then $x^{(2)}_n - 2$ or if $x^{(2)}_n < -1$ then $x^{(2)}_n + 2$

A challenging problem is to synchronize the generator because it exhibits complex nonlinear dynamics. Auto and ring-coupling between states (Fig.4) of the system makes the difficult task to recover the system state on the receiver part from a simple output y. Note that y equals to only one of the states x^p. Moreover, the injection mechanism influence on the dynamics making difficult to predict the region where the points occurs in each next iteration. In addition, chaotic dynamics is quickly reflected by slight changes in parameters e_j. Consequently, observer design requires novel approach application to achieve synchronization.

The next section is devoted to the system parameters identifiability and observability analysis.

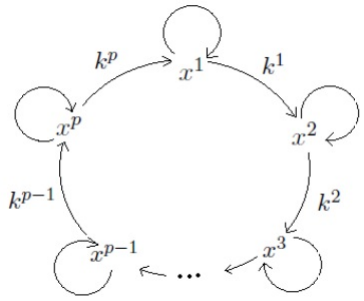


Fig. 4. Auto and ring-coupling between states of the Lozi system

3. IDENTIFIABILITY

3.1. *Identifiability and observability in non-linear (dynamical) system*

For the first time, identifiability of Lozi system with ring- and auto-coupling (1 - 2) is studied. Identifiable parameters are those which affect the value of the data and can be estimated with some degree of certainty. The system is not identifiable:

$$\begin{array}{c} if\ e_1 \neq e_2 \\ y_n(e_1) \neq y_n(e_2) \end{array} \tag{3}$$

A dynamical system is usually first modelled as a system of the following form, called the "state-space" form:

$$x_{n+1} = f(x_n, p, m_n, \sigma)$$

$$y_n = g(x_n, m_n)$$

where $U_n = m_n$ is a vector of input variables (in our case m_n is the message), p is a vector of parameters ($p = \{e_1, e_2, \sigma\}$, $\sigma = session\ key$ is an implicit parameter), x is a vector of state variables (things that cannot be observed or measured directly) while y is the vector of output variables that will be observed (the transmitted signal, in our case).

To analyse strengths and weaknesses of the system (1) we have to answer the questions:

- can we compute m directly from y?
- Are the parameters e_i identifiable or can be computed from U and y (by brute force attack for instance).
- Is the system "observable" or can the values of x be deduced from the value of x, y and their iterates at any time?

Let us consider a simple example of methodology on how to verify the system observability and identifiability for the system:

$$\begin{cases} x^1_{n+1} = \theta x^2_n \\ x^2_{n+1} = 0 \end{cases} \tag{4}$$

To check the identifiability, firstly we have to iterate the system $y_{1,2,3} = m$:

$$\begin{cases} y_n = x^1_n \\ y_{n+1} = \theta x^2_n \\ y_{n+2} = 0 \end{cases}$$

1) The system is observable if the rank is equal to the order:

$$rank \frac{\partial(y_n, y_{n+1}, ..., y_{n+k})}{\partial(x^1_n, x^2_n)} = 2$$

$$rank \begin{bmatrix} 1 & 0 \\ 0 & \theta \end{bmatrix} = 2$$

2) The system is identifiable if the rank is equal to the searched parameters:

$$rank \frac{\partial(y_n, y_{n+1}, ..., y_{n+k})}{\partial \theta} = 1$$

$$rank \begin{bmatrix} 0 \\ x_n^2 \end{bmatrix} = 1$$

3) The system is observable and identifiable if the rank is equal to all unknowns:

$$rank \frac{\partial(y_n, y_{n+1}, ..., y_{n+k})}{\partial(x_n^1, x_n^2, \theta)} = 3$$

$$rank \begin{bmatrix} 1 & 0 & 0 \\ 0 & \theta & x_n^2 \\ 0 & 0 & 0 \end{bmatrix} = 2$$

3.2. *Can we find the secret key (e_i) from the output y?*

If x_n^1 and x_n^2 of the system (1) are known we can find the secret key (epsilons):

$$y_n = \begin{pmatrix} x_n^1 \\ x_n^2 \end{pmatrix} \Rightarrow \frac{\partial y_{n+1}}{\partial(e_1, e_2)} = \begin{bmatrix} x_n^1 - x_n^2 & 0 \\ 0 & x_n^2 - x_n^1 \end{bmatrix} \tag{5}$$

$$\forall_n = \begin{cases} e_1 = \dfrac{x_{n+1}^1 - 1 + 2|x_n^1| - x_n^1}{x_n^2 - x_n^1} \\ e_2 = \dfrac{x_{n+1}^2 - 1 + 2|x_n^2| - x_n^2}{x_n^1 - x_n^2} \end{cases} \tag{6}$$

$Case-1$. When the secret key and only x_n^1 are known. In the model Fig. 10 it is shown that the secret key is exchanged over a secure channel. Thus, we investigate in this case:

$$\begin{cases} y_n = x_n^1 \\ y_{n+1} = 1 - 2|x_n^1| + ((1 - e_1)x_n^1 + x_n^2 e_n)) \end{cases} \tag{7}$$

Consequently, it is possible to find x_n^2

$$\begin{cases} x_{n+1}^1 = y_n \\ x_{n+1}^2 = \frac{y_{n+1} - 1 + 2|y_n| - (1 - e_1)y_n}{e_n} \end{cases} \tag{8}$$

$Case-2$. When the secret key is unknown we have to iterate the system more times because there is one more unknown variable:

$$\begin{aligned} y_{n+2} = 1 - 2\Big|1 - 2|y_n| + [(1 - e_1)y_n + x_n^2 e^n]\Big| + \Bigg[(1 - e_1)\Big\{1 - 2|y_n| + [(1 - e_1)y_n + x_n^2 e_1]\Big\} + \\ + \Big\{[1 - 2|x_n^2| - (1 - e_1)x_n^2 + y_n e_2]e_1\Big\}\Bigg] \end{aligned} \tag{9}$$

Hence, we have to verify if the matrix rank is equal to the number of unknown conditions:

$$\begin{bmatrix} e_1 \\ e_2 \end{bmatrix} = F(y_n, y_{n+1}, y_{n+2}) \tag{10}$$

$$rank \frac{\partial(y_n, y_{n+1}, y_{n+2})}{\partial(e_1, e_2)} = 2 \tag{11}$$

$$rank \begin{bmatrix} 0 & 0 \\ x_n^1 - x_n^2 & 0 \\ \gamma & \delta \end{bmatrix} = 2$$

where

$$\gamma = 2(2 * |x_n^1| - e_1 x_n^1 + x_n^2(e_1 - 1) - 1) * (x_n^1 - x_n^2) + \\ + x_n^1(2|2|x_n^2| + e_2 x_n^2 - x_1^1(e_2 - 1) - 1| - 1)(e_1 - 1) + \\ + e_1 x_n^1(2|2|x_n^2| + e_2 x_n^2 - x_n^1(e_2 - 1) - 1| - 1)$$

$$\delta = -2e_1 x_n^1(2|x_n^2| + e_2 x_n^2 - x_n^1(e_2 - 1) - 1)(x_n^1 - x_n^2)(e_1 - 1)$$

when $e_1 \neq e_2$, $e_j \neq 0$ the system is identifiable.

Our proposition is to raise to a power 2 the epsilons the system (1) to be not identifiable:

$$\begin{cases} x_{n+1}^1 = 1 - 2|x_n^1| + ((1 - e_1^2)x_n^2 + e_1^2 x_n^1) \\ x_{n+1}^2 = 1 - 2|x_n^2| - ((1 - e_2^2)x_n^3 + e_2^2 x_n^2) \end{cases} \tag{12}$$

1) The system is still observable

$$rank \begin{bmatrix} 1 & 0 \\ -2 * (1 - e_1^2) \end{bmatrix} = 2$$

if $e_1 \neq \pm 1,\ \alpha \neq 0$. The system iteration are below:

$$y_n = x_n^1$$
$$y_{n+1} = 1 - 2|x_n^1| + ((1 - e_1^2)x_n^2 + e_1^2 x_n^1)$$

$$y_{n+2} = 1 - 2\Big|1 - 2|y_n| + ((1 - e_1^2)x_n^2 + e_1^2 y_n\Big| + \\ + (1 - e_1^2)\Big(1 - 2|x_n^2| - (1 - e_2^2)x_n^1 + e_2^2 x_n^2\Big)e_1^2 x_n^1$$

where the rank is less than searched parameters:

$$rank \frac{\partial(y_n, y_{n+1}, y_{n+2})}{\partial(e_1, e_2)} = 2 \tag{13}$$

$$rank \begin{bmatrix} 0 & 0 \\ 2(x_n^1 - x_n^2)e_1 & 0 \\ \gamma & \delta \end{bmatrix} = 2$$

where

$$\gamma = 2(2 * |x_n^1| - e_1^2 x_n^1 + x_n^2(e1^2 - 1) - 1) * (2e_1 x_n^1 - 2e_1 x_n^2) + \\ + 2e1^3 x_n^1(2|2|x_n^2| + e_2^2 x_n^2 - x_1^1(e_2^2 - 1) - 1| - 1) + \\ + 2e_1 x_n^1(e_1^2 - 1)(2|2|x_n^2| + e_2^2 x_n^2 - x_n^1(e_2^2 - 1) - 1| - 1)$$

$$\delta = -2e_1^2x_n^1(2|x_n^2| + e_2^2x_n^2 - x_n^1(e_2^2 - 1) - 1)(e_1^2 - 1)(2e_2x_n^1 - 2e_2x_n^2)$$

The epsilons are close to zero, thus the system rank can fall dawn.

3.3. *Section to discuss if identifiability is desirable or not*

Identifiable parameters are those which could be estimated with some degree of certainty. Non-identifiable parameters are those which affect the value of the data, but which cannot be determined accurately. From the security point of view the system should be not identifiable [Xi, F. & Chen, S. & Liu, Z. , 2007], means that the secret key couldn't be recovered from the signal. But in reality, if the system is not identifiable, it is easier to perform brute-force attack. Let us consider a case study of the system: $y_{n+1} = x_n + \alpha^2$, where α is the secret key (according to the definition (eq. 3) it is not identifiable). Hence, the secret key from the output signal cannot be discovered. However, for brute-force attack it is enough to use only positive values that reduce by half ($\frac{1}{2}$) (negative) the choice of the secret key. Thus, it will make the easier task for an intruder.

While the identifiability question rests an open problem, we propose original model with generators shifting. The model is one of the solutions to ensure the secure message transmission either the system is identifiable or non-identifiable.

4. OBSERVER DESIGN

The system (1) exhibits high nonlinear dynamics complicated by injection mechanism. Therefore, observer design requires a particular approach to achieve synchronization. Moreover, the pioneering idea in that paper is to use the system (1) with parameter a that allows to increase executing speed [Garasym O. & Taralova I. , 2013]. The modified Lozi system (15) uses parameter a to change system dynamics according to the binary bit of the message 0/1:

$$a = \begin{cases} 1, m = 1 \\ \omega, m = 0 \end{cases} \tag{14}$$

where m is a message bit equals to "1" or "0", ω is a parameter bounded $[-1, 1]$ and $\omega \neq 0$. Thus, we rewrite (1) with parameter a, such as:

$$\begin{cases} x_{n+1}^1 = 1 - 2|x_n^1| + ak^1((1 - e_1)x_n^2 + e_1x_n^1) \\ x_{n+1}^2 = 1 - 2|x_n^2| + ak^2((1 - e_2)x_n^3 + e_2x_n^2) \\ \vdots \\ x_{n+1}^p = 1 - 2|x_n^p| + ak^2((1 - e_p)x_n^1 + e_px_n^p) \end{cases} \tag{15}$$

The a parameter of the system (15) should be near "1" firstly to support identical statistical properties secondly to avoid determinism. The injection mechanism also has to be fulfilled:

$$\begin{array}{c} \text{if } x_{n+1}^j < -1 \text{ then add } 2 \\ \text{if } x_{n+1}^j > 1 \text{ then substract } 2 \end{array} \tag{16}$$

Observers (Fig. 5) are used on the receiver part to recover x_n, the system states. The knowledge of the system states allows to obtain the same chaotic dynamics on the receiver part as on the transmitter side. To effectively synchronize the system it has to be rewritten from the control point of view (for simplicity we consider the 2nd order system):

$$\begin{cases} x_{n+1} = A_i x_n + B \\ y_n = C_j x_n \end{cases} \tag{17}$$

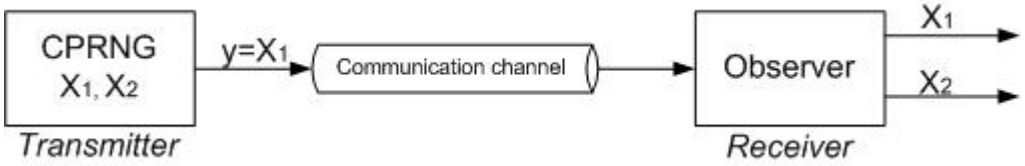


Fig. 5. General model of the system states synchronization by observer application

Where x_n is the state vector, y is the output vector, $B = \begin{bmatrix} 1 \\ 1 \end{bmatrix}$, $C_1 = [1\ 0]$, $C_2 = [0\ 1]$ for $i \in \{1, 4\}$, $j \in \{1, 2\}$ then the system (15) takes the form:

$$\begin{bmatrix} x_{n+1}^1 \\ x_{n+1}^2 \end{bmatrix} = \begin{bmatrix} ae_1 & a(1-e_1) \\ a(-1+e_1) & -e_2 a) \end{bmatrix} \begin{bmatrix} x_n^1 \\ x_n^2 \end{bmatrix} + \begin{bmatrix} ae_1 x_n^1 - 2|x_n^1| + 1 \\ -a(1-e_2)x_n^2 + 1 \end{bmatrix} \begin{bmatrix} 0 \\ -2|x_n^2| \end{bmatrix} \tag{18}$$

$$y_k = [1\ 0]x_n$$

Where $y_n = x_n^1, e_1$ *and* e_2 - are chosen parameters $e_1 = 0.1 \times 10^8, e_2 = 2e_1$ for instance. The system (15) is autonomous discrete-time piece-wise linear system or there are 4 linear states that in effect generate nonlinear dynamics. Consequently, we need four A_i matrices corresponding to the state $[x_1, x_2]$:

$$A_1 = \begin{pmatrix} ae_1 - 2 & a(1-e_1) \\ a(-1+e_2) & -e_2 a - 2 \end{pmatrix} for\ x_1 \in [0, 1]\ and\ x_2 \in [0, 1]$$

$$A_2 = \begin{pmatrix} ae_1 + 2 & a(1-e_1) \\ a(-1+e_2) & -e_2 a - 2 \end{pmatrix} for\ x_1 \in [-1, 0[\ and\ x_2 \in]0, 1[$$

$$A_3 = \begin{pmatrix} ae_1 + 2 & a(1-e_1) \\ a(-1+e_2) & -e_2 a + 2 \end{pmatrix} for\ x_1 \in]-1, 0[\ and\ x_2 \in [-1, 0[$$

$$A_4 = \begin{pmatrix} ae_1 - 2 & a(1-e_1) \\ a(-1+e_2) & -e_2 a + 2 \end{pmatrix} for\ x_1 \in]0, 1[\ and\ x_2 \in]-1, 0[$$

The observability concept for the linear systems is introduced by Kalman under which the system is observable if the rank of the observability matrix O equals to the system's dimension, in our case:

$$rank(O) = rank \begin{pmatrix} C_j \\ C_j A_i \end{pmatrix} = 2$$

$$rank \begin{bmatrix} 1 & 0 \\ -2 + \alpha e_1 & \alpha(1-e_1) \end{bmatrix} = 2$$

for $i \in \{1, 4\}$, $j \in \{1, 2\}$. The system is observable because $0 < \{e_1, e_2\} < 1$ and $a \neq 0$. Consequently, we can build observers in general form:

$$\hat{x}_{n+1} = \hat{A}_i \hat{x}_n + B + K_i^j (\hat{y}_n - y_n) \tag{19}$$

Where $\hat{A}_i$ is a state matrix on the receiver part, $\hat{y}_n$ is the output of the system on the receiver part. The extended Luenberger observer has to be modified as it described in [Espinel, A. & Taralova, I. , 2013]. Even if the states of the system are stable the global dynamic is unstable and for 2-dimension system there are 16 possibilities of point switching. Thus attended Luenberger observer should be applied for each of the regions.

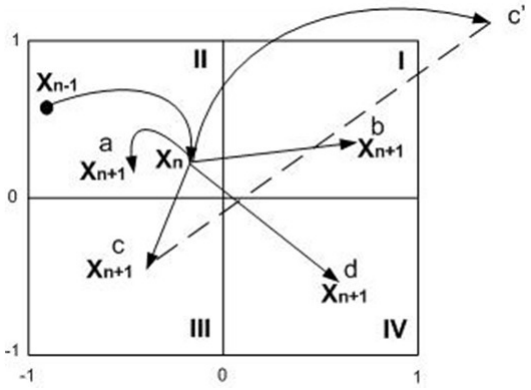


Fig. 6. Possibilities of region switching from x_n point

On the Fig. 6 is also demonstrated that if x_{n-1} fells down to the region II it could switch after to any other locally observable region at the point (b, c, d) or remain to the same region at a. If the point (c) goes out of the interval $[-1,\ 1]^p$ it is feed back by performing equations (16). The novelty here is the double complexity of the system, defined by the state coupling and injection mechanism (16) which makes its influence on the system dynamics.

From control theory it is known that the n-order discrete-time observer converges in n iterations [Moraal, P. & Grizzle, J. , 1995]. We have dealt with 2-dimensional system, so synchronization in 2 steps could be achieved: the first synchronization is performed with x^1_{n+1} and we calculate the error:

$$e_{n+1} = (A_n + K_n C)e_n)$$

on the second with x^2_{n+1} where the error is defined by

$$e_{n+2} = (A_{n+1} + K_{n+1}C)(A_n + K_n C)e_n$$

Stable observer design requires K-matrix respecting the region of x_n. Thus for each region A_i with $i \in \{1, 4\}$, $j \in \{1, 2\}, C[1\ 0]$, we have K^j_i matrices:

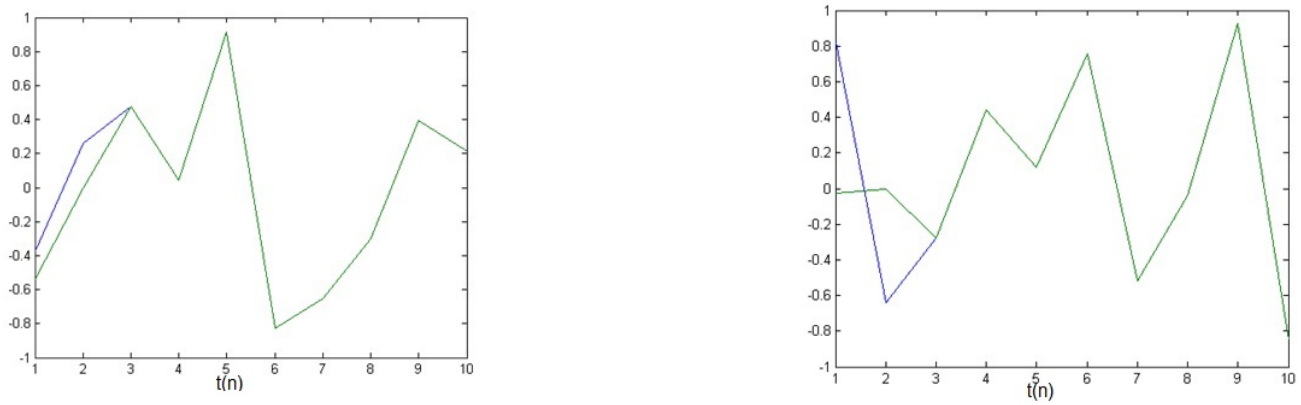
$$K^1_1 = \begin{pmatrix} 4 - ae_1 + ae_2 \\ \frac{4-a^2+a^2e_1+4ae_2+a^2e_1e_2+a^2e_2^2}{a(-1+e_1)} \end{pmatrix} \qquad K^1_3 = \begin{pmatrix} -4 - ae_1 + ae_2 \\ \frac{4-a^2+a^2e_1-4ae_2+a^2e_2-a^2e_1e_2+a^2e_2^2}{a(-1+e_1)} \end{pmatrix}$$

$$K^1_2 = \begin{pmatrix} -ae_1 + ae_2 \\ -\frac{4+a^2-a^2e_1-a^2e_2+a^2e_1e_2-a^2e_2^2}{a(-1+e_1)} \end{pmatrix} \qquad K^2_3 = \begin{pmatrix} -ae_1 + ae_2 \\ -\frac{4+a^2-a^2e_1-a^2e_2+a^2e_1e_2-a^2e_2^2}{a(-1+e_1)} \end{pmatrix}$$

$$K^2_1 = \begin{pmatrix} -ae_1 + ae_2 \\ \frac{4-a^2+a^2e_1+4ae_2+a^2e_2-a^2e_1e_2+a^2e_2^2}{a(-1+e_1)} \end{pmatrix} \qquad K^1_4 = \begin{pmatrix} -ae_1 + ae_2 \\ \frac{4-a^2+a^2e_1-4ae_2+a^2e_2-a^2e_1e_2+a^2e_2^2}{a(-1+e_1)} \end{pmatrix}$$

$$K^2_2 = \begin{pmatrix} -4 - ae_1 + ae_2 \\ -\frac{4+a^2-a^2e_1-a^2e_2+a^2e_1e_2-a^2e_2^2}{a(-1+e_1)} \end{pmatrix} \qquad K^2_4 = \begin{pmatrix} -4 - ae_1 + ae_2 \\ -\frac{4+a^2-a^2e_1-a^2e_2+a^2e_1e_2-a^2e_2^2}{a(-1+e_1)} \end{pmatrix}$$

The message bits recovery could be performed on the receiver part after the synchronization is achieved. On the Fig. 7 synchronization result for x_1 is demonstrated. Transmitter and receiver trajectories become to be identical in only two iterations.



a) b)

Fig. 7. Synchronization results of a) x_1 *and* $\hat{x}_1$ b) x_2 *and* $\hat{x}_2$

High precision in synchronization mode could be obtained when x_1 and x_2 for two-dimensional system have minimal error:

$$e_n = \sqrt{(x_n^1 - \hat{x}_n^1)^2 + (x_n^2 - \hat{x}_n^2)^2}$$

graphical synchronization error results are on the Fig. 8.

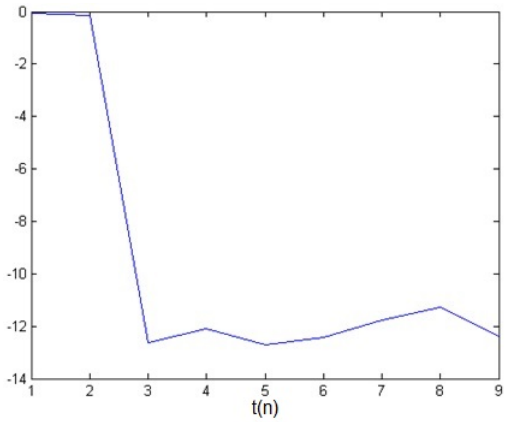


Fig. 8. Synchronization error

However, the observer design is a necessary but not sufficient condition for secure message transmission. Next sections are devoted to the original encryption scheme that improves the security.

5. CSK MODEL WITH IMPLEMENTED CHAOTIC SHIFTING

The CSK breaking methods are based on the detection of the signal dynamics differences [Yang, T. & Yang, L. & Yang, C. , 1998]. Changes in signal dynamic mean switching between bits 0 and 1. This new method has to ensure encryption process: firstly, with uniform dynamics otherwise the original message (information) will be easily recovered; secondly, even if generators switching is detected, it shouldn't indicate switching between bits.

The first requirement is satisfied using chaotic system (15). To solve the second problem we propose to use z-order shifting generators, where $z \geq 3$. Note, the more amount z of generators are used, the larger number of possible combinations is.

This idea provides advantages:

- Increases security level. The use of several shifting generators where each of them implies non-linear dynamics with similar spectral and statistical properties complicates general system dynamics.
- Resolves CSK weakness. Even if the generator's switching has been detected it does not correspond to message bits. Thus it is impossible to break the encryption model by switching regimes detection (change $1 \Rightarrow 0$ or $0 \Rightarrow 1$). Moreover, shifting between 2-dimensional chaotic systems is sufficient to reach satisfied randomness.
- Increases speed performance. Synchronization could be achieved in only 2 steps for 2-dimensional system. Moreover, a parameter allows quickly switch between generators.
- Preserves robustness of the CSK model against noise.

5.1. *Original CSK model description*

The observer have been successfully designed (section 4) for the chaotic generator (15). Thus, we can do detail analysis of the original model. The original idea is to use z-chaotic generators and shift them according to the session key at each iterating. The main advantage is the improved security since the same generator can be used to encrypt 0 or 1, depending on the session key. Session key is a single-use symmetric key applied for message encryption in one communication session [Kocher, P. , 2011]. We propose to use chaotic shifting combination as a session key.

Let us consider the following example with 3 shifting generators (Fig. 9, Table 1). Switching between 2 always active generators is realized according to the message bit 1/0. Session key indicates which generators are active in the current iteration. At each iteration, the bit encryption is performing as in the traditional CSK model by switching between two active generators according to the bit. At each iteration generators also are shifting according to the session key (generators order).

For instance, session key $1 \Rightarrow 2 \Rightarrow 3$ means that generators 1 and 2 are active at time t, then 2 and 3 are active at $t+1$ etc. The first generator (G1) with parameter $a = 1$, the second (G2) with $a = 0.1$, the third (G3) with $a = -1$. Moreover session key $1 \Rightarrow 2 \Rightarrow 3$ means also that at the first iteration G1 corresponds to the bit "1" and G2 to the bit "0", G3 is inactive. If the message is represented in binary form: "1000" then we use G1 to encrypt "1" at the first iteration, for the next bit "0" G1 is used as well because of generators switching order, the next "0" $\rightarrow G3$, next "0" $\rightarrow G2$ by the same principle.

At each iteration only 2 generators are active. Moreover, the generator shifting order is considered as the additional parameter (selected by chaotic generator). Note that, session key has to be concerted over secure channel.

Table 1. Original CSK model encryption process

Generator	t	t+1	t+2
G1	1	0	inactive
G2	0	inactive	1
G3	inactive	1	0

The example demonstrates that even if switching regimes were detected it doesn't mean switching between bits "0" and "1". The example shows that at time $t+1$, G1 was used to encrypt the bit "0". However, at the next $t+2$, G3 was used to encrypt also bit "0". Thus, generated dynamics was changed, but the same bit "0" was encrypted. Moreover, if the same generator is used for encryption it doesn't mean that at that time the same bit is encrypted. It is demonstrated in example when at time t, G1 was used

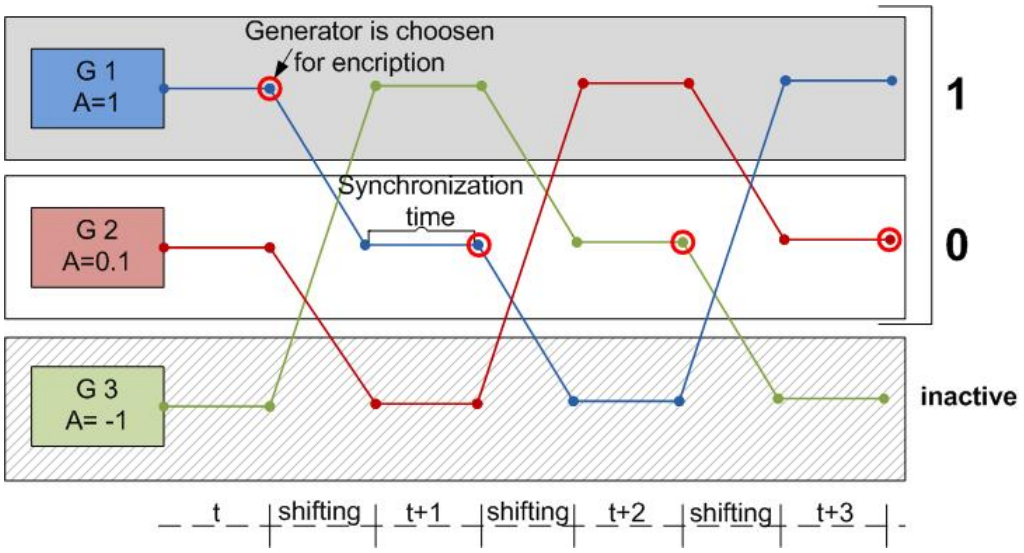


Fig. 9. Chaotic generators cycle switching and shifting

to encrypt message bit "1" and at the next $t+1$, also G1 was used but to encrypt bit "0". Thus, there is no changes in generated dynamics because the same generator was used however to encrypt different bits. The proposed chaotic encryption approach significantly increases security of the CSK model.

5.2. *Implementation original CSK model to symmetric encryption algorithm*

Let us consider the implementation original CSK model to symmetric encryption method (Fig. 10). The method uses the secret key with which both parts (transmitter and receiver) exchange confidential information. the secret parameters are used to encrypt/decrypt the message. The main purpose of the symmetric encryption algorithms is high-speed encryption of large amounts data [Garasym O. & Taralova I. , 2013]. In our case of 2-dimension system (15) the secret key are initial conditions (e_1, e_2, a, x_0) of the system (15). Moreover, the proposition to use z-order shifting generators plays two crucial roles. Firstly, to increase the security level of the transmitted signal, secondly it is used as a session key. The original encryption CSK model with session and encryption keys exchange is demonstrated on the Fig. 10.

Note that, the session key needs to be exchanged between two communicating parties in a secure way. An example is to use public-key cryptographic algorithms such as RSA or elliptic curve cryptography (ECC) to exchange a 128-bit session key for use in Advanced Encryption Standard (AES) symmetric-key ciphers. However, it is not the purpose of the paper but could be found in the reference [Yang, J. & Seo, C. & Cho, J. , 2007].

Transmitter and receiver are exchanging the secret key $(e_1, e_2, ..., e_n)$ over the secure channel and match up the session key (Fig.10). The message is converted into a binary form. Two generators are used for encryption one bit 0/1 as it is proposed in the general model and the third chaotic generator is non-active. The generators are changing their order in each next bit to ensure secure transmission. In this case the same generator could encrypt bit "1" and "0" as it was described earlier. Encrypted message (cipher text) (Fig.10) is transmitted over the insecure channel. On the receiver part, observers are used to decrypt the message. For message encryption only one of the states is used (for ex. x^1, Fig.5) and transmits over the communicational channel. From the output y, observer recovers all systems states for successful synchronization performing.

One observer (the system sates reconstruction) application is enough in theory for CSK model to recover the message. The observer performs full chaotic synchronization, and if the error diverges from 0, the "1" bit is indicated otherwise "0". In real life, two different observers are used because existence of noise in the communication channel influences qualitative synchronization, and both would be divergent from 0. Consequently, the errors are compared after the observers reach a full chaotic synchronization. The smallest error indicates which generator has been used for the bit encryption (Fig. 11).

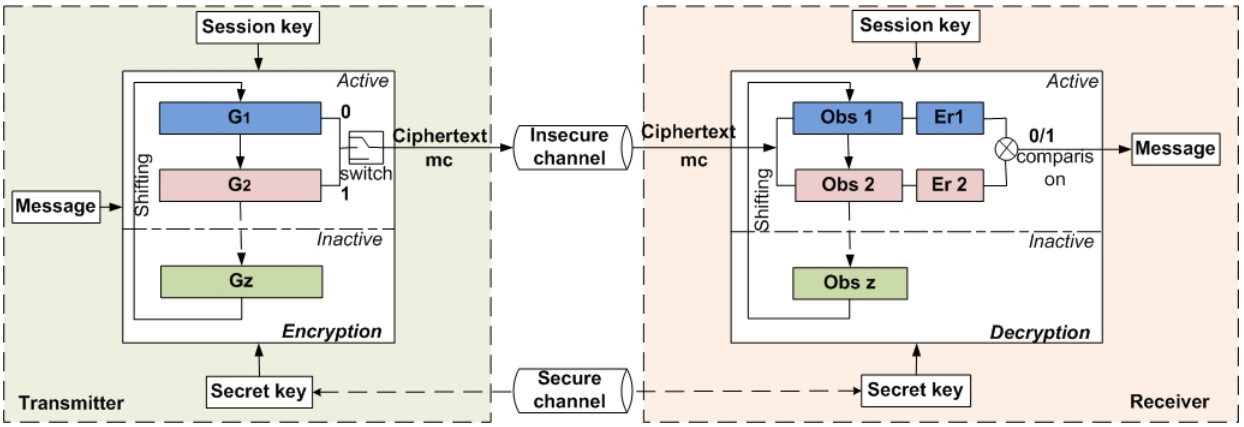


Fig. 10. Symmetric encryption algorithm with implemented original CSK model for secure message transmission

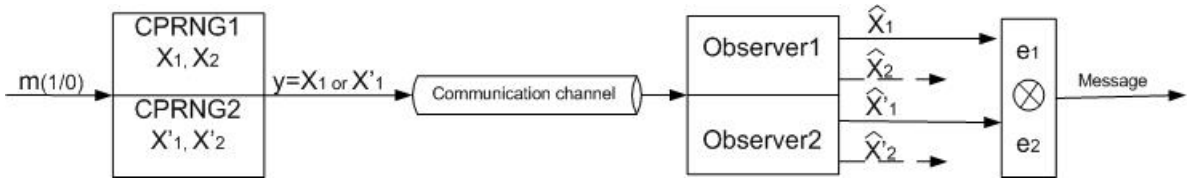


Fig. 11. Message recovery by using two chaotic observers

The original CSK model also requires two active observers to recover the message where smaller error indicates generator that was encrypted the bit (Fig. 12). Observers are changing the order on the next iteration according to the session key.

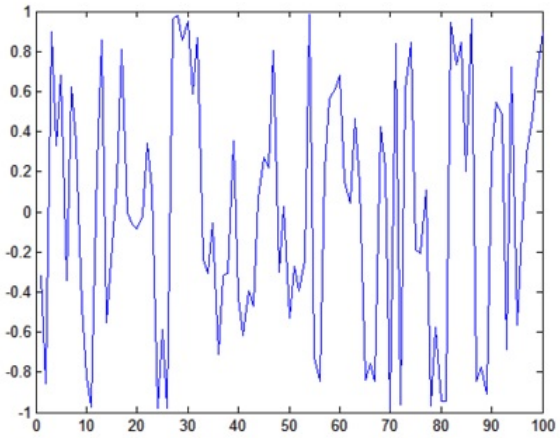


Fig. 12. The signal of encrypted message m_c

One of the information security requirements is message decryption. The encryption method is pointless if it is impossible to recover the message. The successful message recovering by errors comparison depends on hight precision of the synchronization.

6. RELIABILITY TESTS OF THE ORIGINAL CSK MODEL

In this section, several tests of the model reliability are demonstrated: sensitivity to initial conditions and session key; NIST tests of the encrypted signal; correlation between wrong decrypted messages; system ergodicity.

Note that, each of the generators is independent of the others. The parallel switches depend on the session key but also on the message itself. Thus, for each different message (i.e. different binary sequences), there will be different output. Moreover, the session key (generated by another chaotique generator) depends on each communication (run). The session key is generated by another chaotic generator to avoid brute-force attack.

For the experiments 3 generators were taken as the most critical combination. However, in practice it is recommended to use more generators to minimise the risk of brute-force attack. Note that, the increasing number of generators increases security but has not influence on speed performance and is as simple in implementations as in the case of 3 generators.

(1) System sensitivity to initial conditions.
On the (Fig.13) it is shown an example where the generator structure, session key (chaotic switching order), epsilons are known on the both sides of the communication channel except one epsilon of the generator $G1$ out of tree. The epsilon has slightly other parameter ($e_1 = 0.100001$ instead of 0.1). The model quickly reacts to any changes. Thus, the error in the initial condition only of one of the generators leads to wrong message recovery (Fig.14).

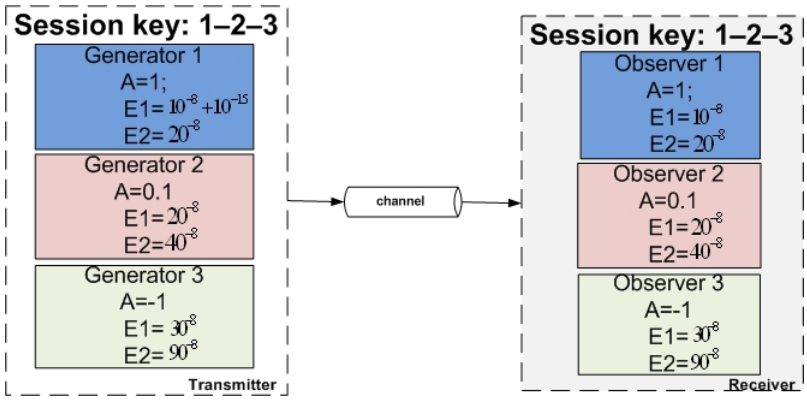


Fig. 13. Slightly different secret key error at the first generator

a) b)

Fig. 14. Decryption results while the secret key error a) plain text b) wrong decryption

(2) System sensitivity to error in the session key.
For the original CSK model with z-number shifting generators, there are $z!$ possibilities of the seance keys. If the key is wrong (Fig.15) the message recovery leads to strongly different results as it have to (Fig.16). Numerous generators could be easily implemented and do not influence to speed performance.
(3) Correlation between wrong decrypted messages.
Moreover, errors in session keys do not correlated to each other. The results of unknown session keys lead to totally different messages decryption (Fig. 17).
(4) Shifting test.
On the Fig. 18 it is shown that each of the generators is used to encrypt bit "1" and "0" or rest

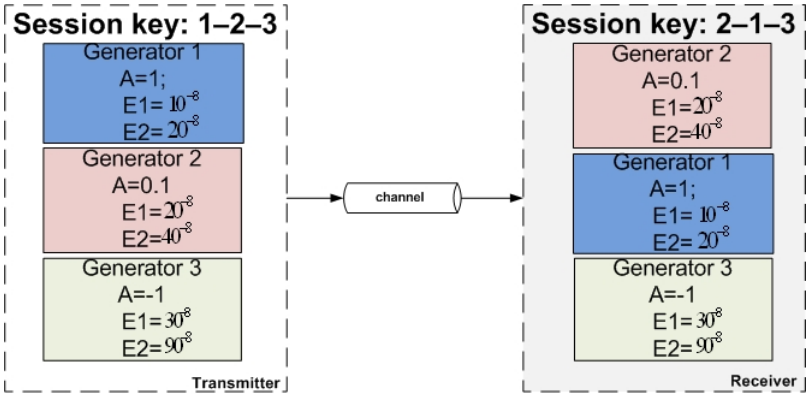
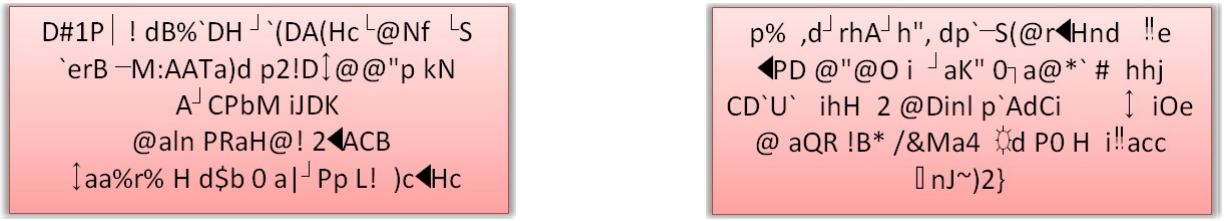


Fig. 15. Slightly different secret key error at the first generator

a) b)

Fig. 16. Decryption results while the session key error a) plain text b) wrong decryption



a) b)

Fig. 17. Errors in the session key do not correlate to each other a)incorrect session key (2-1-3) b) incorrect session key (3-1-2)

non-active ”-1”. Such method improves the model security because even if it will be detected switching generators regimes it won’t break encryption.

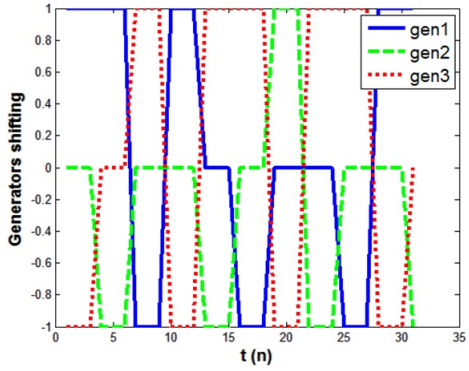


Fig. 18. The generators shifting while the message encryption is performing

(5) System ergodicity.
The model advantage is also that the transmitted signal is ergodic. It means that even if the session key and/or initial conditions are different but the system behavior is preserved, demonstrating nearly the same histogram in all cases. The importance is based on the preventing illegal message recovery by histogram comparison of the messages, where $m_1 = 00000$ (only zeros)and $m_2 = 11111$ (only ones). For the experiment 10^5 bites were generated with session key $1 \Rightarrow 2 \Rightarrow 3$. The approximate density function [Lozi, R. , 2012] has been used as more demonstrative for the system analyzes. The graph of the chaotic attractor was divided for 20×20 "boxes" and points in it were calculated (Fig. 19).

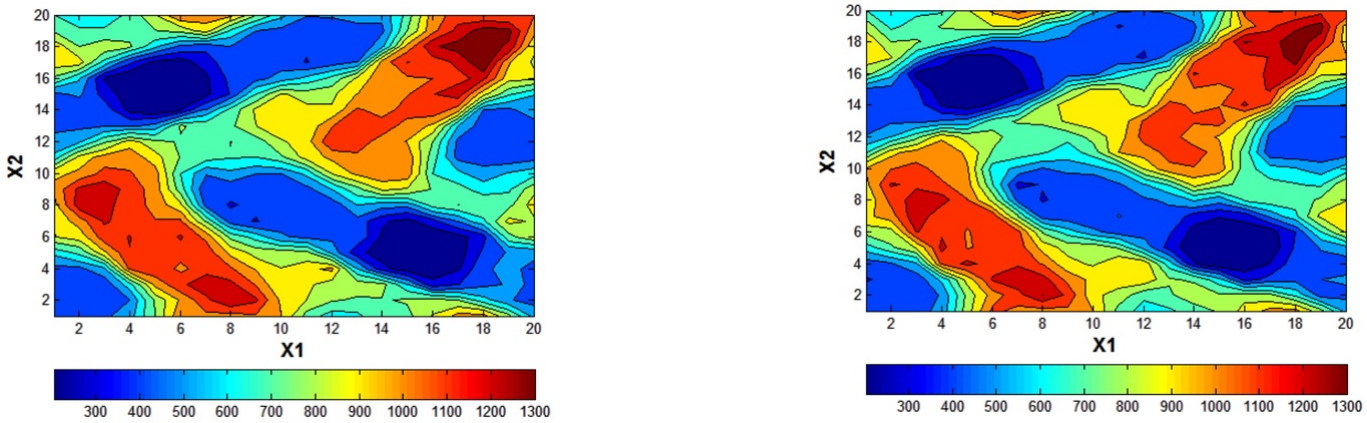


Fig. 19. Approximate density function for encrypted message m_c (10^5 bites) in the chaotic signal where a)all bits of the message m are 0 b) all bits of the message m are 1

(6) NIST tests for randomness [Rukhin, A. & Soto, J. , 2010].
The sequences of the 3 shifting generators model is checked for randomness by NIST tests to prove secure signal transmission. The original CSK model has been applied to encrypt 4×10^6 randomly produced bits. The results of the successfully passed NIST tests are represented in the table 2.

Table 2. Successful NIST tests of the transmitted signal

Test Name	Proportion of the successful tests
Frequency	98/100
BlockFrequency	97/100
CumulativeSums	98/100
Runs	99/100
LongestRun	100/100
Rank	98/100
FFT	98/100
NonOverlappingTemplate	99/100
OverlappingTemplate	98/100
Universal	98/100
ApproximateEntropy	99/100
RandomExcursions	61/61
RandomExcursions Variant	61/61
Serial	98/100
LinearComplexity	100/100

7. CSK, SM, OCSK models comparison

Progress has been made to the point that chaos can be applied to secure communication [Feki, M. , 2003; Zaher, A. & Abu-Rezq, A. , 2011] and many papers focused on robust chaotic generator design [Dogan, R. & Murgan, A. , 1996; Banerjee, S. & Kastha, D. & Das, S. , 1999; Katz, O. & Ramon, D. & Wagner, I. , 2008]. There are several criteria respected by the community to the chaotic generators: Largest Lyapunov exponent [Sato, S. & Sano, M. & Sawada, Y. , 1987], Chaotic attractor in the phase space [Dowell, E. & Pezeshki, C. , 1986; Hartley, T. & Lorenzo, C. & Killory Q. , 1995], phase delay [Liebert, W. & Schuster, H. , 1989; Fyodorov, Y. & Sommers, H. & others , 1997], Topologically mixing [Jincheng, X. & Zhongguo, Y. , 1991; Thiffeault, J. & Finn, M. , 2008], Reactivity to small changes in initial conditions (chaotic sensitivity) [Sudret, B. , 2008; Banks, J. & Brooks, J. , 1992], Uniform distribution [Hong, Z. & Xieting, L. , 1997; Dachselt, F. & Schwarz, W. , 2001], Autocorrelation [Frey, D. , 1993; Hong, Z. & Xieting, L. , 1997], Crosscorrelation [Heidari-Bateni, G. & McGillem, C. , 2013], NIST tests [Wang, S. & Kuang, J. , 2002; Rukhin, A. & Soto, J. , 2010]. Short description each of the criteria is given bellow:

C1 - Positive Largest Lyapunov exponent (LLE). A positive largest Lyapunov exponent indicates chaotic behavior and the value of this index defines the chaoticity degree: the larger is LLE, the stronger chaotic dynamics exhibits the system. LLE characterizes the average rate of exponential divergence of closely initialised phase trajectories consequently it demonstrates sequences unpredictability in short-term.

C2 - Chaotic attractor in the phase space (dense everywhere). Phase plot (space) is a space in which all possible states (dimensions) of a system are represented at trajectory (x_n^i, x_n^j), with each possible state of the system is relevant to one unique point in the phase space. The phase space graph signifies good randomness if the probability of the scattered points is uniformly distributed.

C3 - Chaotic attractor in phase delay (dense everywhere). Delay plot (recurrence plot) is very close to the phase space but is used only for one dimension of the system. Delay plot is represented by cartography of the chaotic attractor with time delay (x_n^i, x_{n+1}^i). The phase delay graph indicates good randomness if the probability of the scattered points is uniformly distributed.

C4 - Topological mixing. Topological mixing in the theory of chaos means a system extension when one part of the attractor at some moment is superimposed on any other part of the area.

C5 - Reactivity to small changes in initial conditions. A slight change in initial parameters leads to generating new random sequences. The shorter time of the transient period the system exhibits the better reactivity is.

C6 - Uniform distribution. Distribution histograms allow to estimate samples partition in the studied sequence and to determine the frequency of occurrence of a particular distribution value. For the random sequences, the frequency character should be about the same.

C7 - Autocorrelation (near zero). Autocorrelation function is used as a qualitative tool for checking randomness. The random sequence has autocorrelations near zero for all time-lag. If one or more of the autocorrelations sharply deviate from zero, it indicates non-randomness except one autocorrelation peak when the shift equals to the signal length.

C8 - Crosscorrelation (near zero). The cross correlation function measures the dependence of the values of one signal x_n^1 on another x_n^2.

C9 - NIST tests (successful). NIST statistical tests are used as a tool to verify sequences produced by generator for randomness. For each test, a conclusion is drawn about acceptance or refusal.

As it has been summarized in the scheme (Fig.20) each of the criteria should be successfully passed otherwise the system can't be used in cryptography.

The described criteria were used to study chaotic generators dynamics however this research is focused on the entire model dynamics. To our best knowledge we are the first who studies system dynamics in a whole when several generators are applied. The objectives are to acquire knowledge how to increase signal complexity and security, what type of chaotic generators could be combined and which initial conditions have to be chosen. The software has been designed (Figs.21, 22).

In order to assess numerical computations more accurately and to qualitatively compare the systems by criteria C2, C3 and C6, an approximation density function is applied. The approximation $P_{M,N}(x)$ is defined of the invariant measure (the probability distribution function) linked to the 1-dimensional map f,

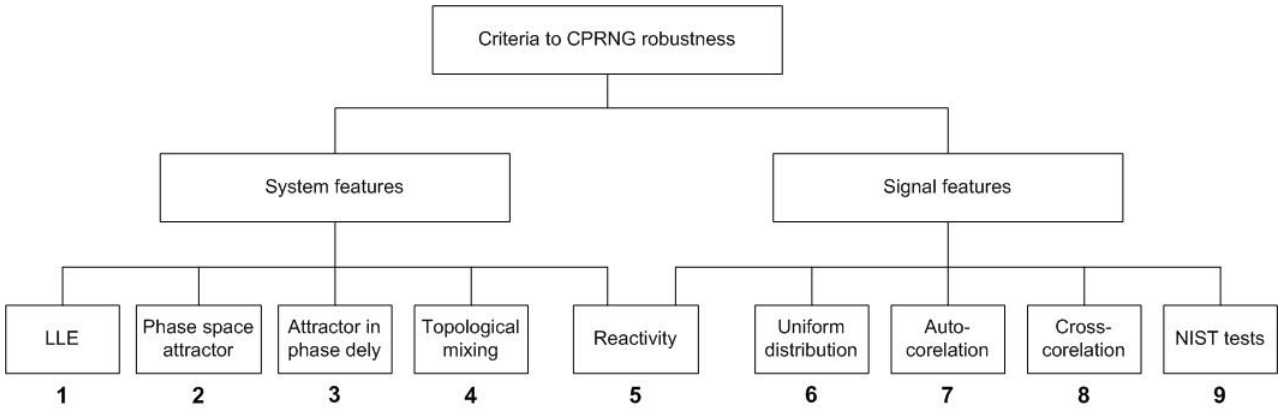


Fig. 20. Criteria for chaotic PRNG design

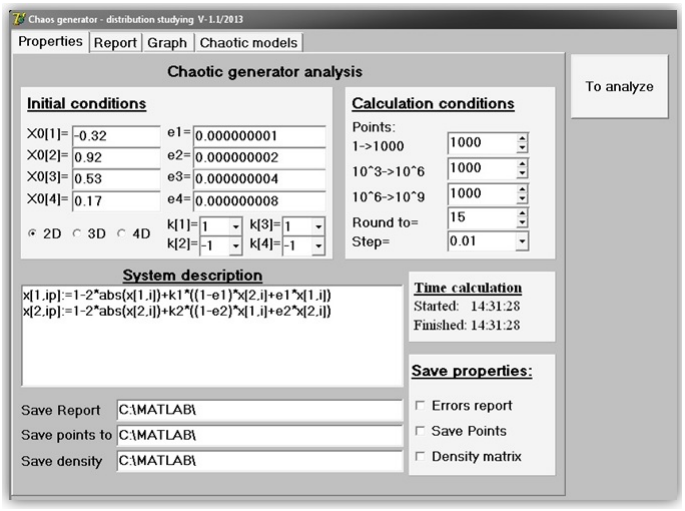


Fig. 21. Software design to chaotic signal analysis

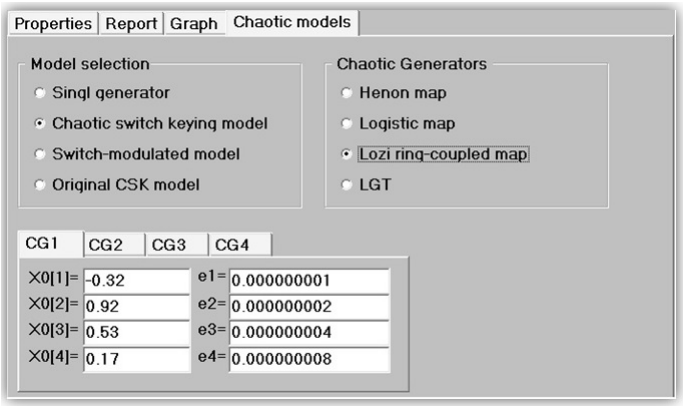


Fig. 22. Selection chaotic generator, model and initial conditions in the software to signal analysis

when computed with floating numbers [Lozi, R. , 2009]. The regular partition of M small intervals (boxes) r_i of J is defined by

$$s_i = -1 + \frac{2i}{M}, i = 0, M \tag{20}$$

$$r_i = [s_i, s_{i+1}[\quad i = 0,\ M-2 \ and\ r_{M-1} = [s_{M-1}, 1] \tag{21}$$

the length of each box is equal to $\frac{2}{M}$ and the r_i intervals form a partition of the interval J

$$J = \bigcup_{0}^{M-1} r_i \tag{22}$$

All iterates $f^{(n)}(x)$ belonging to these boxes are collected, after a transient regime of Q iterations decided *a priori*, (i.e. the first Q iterates are neglected). Once the computation of $N+Q$ iterates is completed, the relative number of iterates with respect to N/M in each box r_i represents the value $P_N(s_i)$. The approximated $P_N(x)$ defined is then a step function, with M steps. As M may vary, it is defined

$$P_{M,N}(s_i) = \frac{M}{N}(\sharp r_i) \tag{23}$$

where $\sharp r_i$ is the number of iterates belonging to the interval r_i. $P_{M,N}(x)$ is normalized to 2 on the interval J.

$$P_{M,N}(x) = P_{M,N}(s_i), \forall x \in r_i \tag{24}$$

The system (1) is combined of p-coupled maps, thus it is important to analyse distribution of each component $x^1, x^2, x_1^2, ..., x^p$ of X and variable X itself in J^p as well. The approximated probability distribution function , $P_{M,N}(x^j)$ associated to one among several components of $F(X)$. It is used equally N_{disc} for M and N_{iter} for N, when they are more explicit.

The discrepancies E_1 (in norm L_1), E_2(in norm L_2) and E_∞ (in norm L_∞) between $P_{N_{disc},N_{iter}}(x^j)$ and the Lebesgue measure, which is the invariant measure associated to the symmetric tent map, are defined by

$$E_{1,N_{disc},N_{iter}}(x^j) = \|P_{N_{disc},N_{iter}}(x^j) - 1\|_{L_1} \tag{25}$$

$$E_{2,N_{disc},N_{iter}}(x^j) = \|P_{N_{disc},N_{iter}}(x^j) - 1\|_{L_2} \tag{26}$$

$$E_{\infty,N_{disc},N_{iter}}(x^j) = \|P_{N_{disc},N_{iter}}(x^j) - 1\|_{L_\infty} \tag{27}$$

All tests are of large scale, therefore we propose to consider the summary table (Table 3). In the table chaotic switch keying (CSK), switch-modulated (SM) [Wang, X. & Gao, Y. , 2010] and Original CSK (OCSK) are compared by criteria C1-C9, encryption time, decryption time, robustness against noise, reliable against switching regimes detection. For the last tests the model breaking method when the observers have different initial conditions from the conditions on the transmitter part was used [Yang, T. & Yang, L. & Yang, C. , 1998].

The model signal dynamics depends on, primarily, from the generators are applied in it thats why the models are successfully passed the tests on criteria C1-C9 with no significant differences. Thus, we define (+) when the system has the best statistical properties, (+-) or (-) if the results are worse. The firm side of the CSK model as it was described earlier is robust against noise, while security level is low (-). The best feature of the SMM model is encryption time performing because the model encrypts by pair bits, nevertheless the model requires 4 active observers on the receiver part that is time-consuming.

Table 3. CSK, SM, OCSK models comparison

Test Name	CSM	SM	OCSK
Largest Lyapunov exponent	0.655	0.6552	0.6564
Chaotic attractor in the phase plane	+-	+	+
Chaotic attractor in phase delay	+-	+	+
Topologically mixing	+-	+-	+
Reactiveness to small changes in IC	+	+	+
Uniform distribution	+-	+	+
Autocorrelation	+	+	+
Crosscorrelation	+	+	+
NIST tests	-	+-	+
Encryption time (1000 bits)	1.589758	0.97418	1.596321
Decryption time (1000 bits)	1.460496	1.454114	1.472562
Robustness against noise (variance)	10^{-5}	10^{-21}	10^{-5}
Switching regimes detection	-	-	+

Consequently, total encryption/decryption time is nearly the same of the CSK, SMM and OCSK models. Even if signal complexity of the SMM model is higher than in CSK model but it also exhibits weakness against switching regimes detection attacks (-). The OCSK model demonstrates high signal complexity, secure level; the model is reliable against switching regimes detection attacks, preserves CSK model advantage: the robustness against noise. We would like to emphasise that CSK and OCSK models perform full correct message recovery while noise variance is 10^{-5} comparing with SMM where noise variance should be no more than 10^{-21}.

8. CONCLUSION

This paper is focused on improving security level of the classical CSK model. The identifiability and observability have been discussed as necessary (but not sufficient) conditions for successful secure synchronization. The proposed original idea of z-generators shifting exhibits more complex signal dynamics and solves the problem of switching regimes detection. Number of generators that are implemented in the model should be sufficient to avoid brute-force attack. However, number of generators does not influence speed performance and is simple in implementation. Transmitter signal as an example with 3 shifting generators has been successfully verified for robustness by: sensitivity to initial conditions and session key; NIST tests; correlation between wrong decrypted messages; system ergodicity. The paper provides the observer design to autonomous discrete-time piece-wise linear chaotic system implying only 2 steps to reach synchronization. Further research is concentrated on the system dynamics study while structurally different chaotic generators are applied.

References

Anstett, F. & Millerioux, G. & Bloch, G. [2006] *Chaotic cryptosystems: Cryptanalysis and identifiability*, Circuits and Systems I: Regular Papers, IEEE Transactions on, vol. 53, pp. 2673–2680.

Banerjee, S. & Kastha, D. & Das, S. & Vivek, G. & Grebogi, C. [1999] *Robust chaos-the theoretical formulation and experimental evidence*, Circuits and Systems, 1999. ISCAS'99. Proceedings of the 1999 IEEE International Symposium on, vol. 5, pp. 293–296.

Banks, J. & Brooks, J. & Cairns, G. & Davis, G. & Stacey, P. [1992] *On Devaney's definition of chaos*, American Mathematical Monthly, vol. 11, pp. 332–334.

Dedieu, H. & Ogorzalek, M. [1997] *Identifiability and identification of chaotic systems based on adaptive synchronization*, Circuits and Systems I: Fundamental Theory and Applications, IEEE Transactions on, vol. 44, pp. 948–962.

Dedieu, H. & Ogorzalek, M. [1995] *Identification and control of a particular class of chaotic systems*, Photonics East'95, pp. 148–156.

Dachselt, F. & Schwarz, W. [2001] *Chaos and cryptography*, IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications, vol. 48, pp. 1498–1509.

Dogan, R. & Murgan, A. & Ortmann, S. & Glesner, M. [1996] *Searching for robust chaos in discrete time neural networks using weight space exploration*, Neural Networks, 1996., IEEE International Conference on, vol. 2, pp. 688–693.

Dowell, E. & Pezeshki, C. [1986] *On the understanding of chaos in Duffings equation including a comparison with experiment*,Journal of Applied Mechanics, vol. 1, pp. 5–9.

Espinel, A. & Taralova, I. [2013] *Ring-Coupled Chaotic Generator for Coherent and Non-Coherent Detection*, Adaptation and Learning in Control and Signal Processing, vol. 11, pp. 718–723.

Feki, M. [2003] *An adaptive chaos synchronization scheme applied to secure communication*, Chaos, Solitons & Fractals, vol. 18, pp. 141–148.

Frey, D. [1993] *Chaotic digital encoding: an approach to secure communication*, Circuits and Systems II: Analog and Digital Signal Processing, IEEE Transactions on, vol. 40, pp. 660–666.

Fyodorov, Y. & Sommers, H. & others [1997] *Statistics of resonance poles, phase shifts and time delays in quantum chaotic scattering for systems with broken time reversal invariance*, arXiv preprint cond-mat/9701037, vol. 11.

Garasym, Oleg & Taralova, Ina [2013] *High-speed encryption method based on switched chaotic model with changeable parameters*, Information Science and Technology (ICIST), 2013 International Conference on, pp. 37–42.

Hartley, T. & Lorenzo, C. & Killory Q. [1995] *Chaos in a fractional order Chua's system*, Adaptation and Learning in Control and Signal Processing, vol. 42, pp. 485–490.

Hasan, M. & Idris, I. & Uddin, A. & Shahjahan, M. [2012] *Performance analysis of a coherent chaos-shift keying technique*, Computer and Information Technology (ICCIT), 2012 15th International Conference on, pp. 249–254.

Hasler & Martin [1998] *Chaos shift keying in the presence of noise: A simple discrete time example*, Circuits and Systems, 1998. ISCAS'98. Proceedings of the 1998 IEEE International Symposium on, vol.3, pp. 271–274.

Heidari-Bateni, G. and McGillem, C. [2013] *A chaotic direct-sequence spread-spectrum communication system*, Communications, IEEE Transactions on, vol. 42, pp. 1524–1527.

Heil, T. & Mulet, J. & Fischer, I. & Mirasso, C. & Peil, M. & Colet, P. & Elsasser, W. [2002] *ON/OFF phase shift keying for chaos-encrypted communication using external-cavity semiconductor lasers*, Quantum Electronics, IEEE Journal of, vol. 38, pp. 1162–1170.

Hong, Z. & Xieting, L. [1997] *Ring-Coupled Chaotic Generator for Coherent and Non-Coherent Detection*, Adaptation and Learning in Control and Signal Processing, vol. 7, pp. 205–213.

Jincheng, X. & Zhongguo, Y. [1991] *Ring-Coupled Chaotic Generator for Coherent and Non-Coherent DetectionChaos caused by a topologically mixing map*,International Centre for Theoretical Physics, Trieste (Italy).

Katz, O. & Ramon, D. & Wagner, I. [2008] *A robust random number generator based on a differential current-mode chaos*, Very Large Scale Integration (VLSI) Systems, IEEE Transactions on, vol. 16, pp. 1677–1686.

Kocher, P. [2011] *Payment smart cards with hierarchical session key derivation providing security against differential power analysis and other attacks*, Google Patents, US Patent 7,941,666.

Liebert, W. & Schuster, H. [1989] *Proper choice of the time delay for the analysis of chaotic time series*, Physics Letters A, vol. 142, pp. 107–111.

Liang, X. & Zhang, J. & Xia, X. [2008] *On the application of parameter identifiability to the security of chaotic synchronization*, Intelligent Control and Automation, 2008. WCICA 2008. 7th World Congress on, vol. 142, pp. 508–512.

Liu, J. & Zhang, Y. [2011] *The application of Chaotic masking and chaotic switching in communication*, 2011 Second International Conference on Mechanic Automation and Control Engineering, pp. 7781–7784.

Lozi, R. [2012] *Emergence of randomness from chaos*, International Journal of Bifurcation and Chaos, v. 22, 2, pp. 1250021–1/15.

Lozi, R. [2009] *Chaotic pseudo random number generators via ultra weak coupling of chaotic maps and double threshold sampling sequences*, Proceeding of the 3rd Conference on Complex Systems and

Applications, University of Le Havre, France, June 29-July 02 (2009), C. Bertelle, X. Liu, MA Aziz-Alaoui (eds.), pp. 20–24.

Moraal, P. & Grizzle, J. [1995] *Observer design for nonlinear systems with discrete-time measurements*, Automatic Control, IEEE Transactions on, vol. 40, pp. 395–404.

Rukhin, A. & Soto, J. & Nechvatal, J. & Barker, E. & Leigh, S. & Levenson, M. & Banks, D. & Heckert, A. and Dray, J. and Vo, San and others [2010] *Statistical test suite for random and pseudorandom number generators for cryptographic applications, NIST special publication*, Statistical test suite for random and pseudorandom number generators for cryptographic applications, NIST special publication.

Sato, S. & Sano, M. & Sawada, Y. [1987] *Practical methods of measuring the generalized dimension and the largest Lyapunov exponent in high dimensional chaotic systems*, Progress of Theoretical Physics, vol. 77, pp. 1–5.

Sudret, B. [2008] *Global sensitivity analysis using polynomial chaos expansions*, Reliability Engineering & System Safety, vol. 93, pp. 964–979.

Terry, J. & VanWiggeren, G. [2001] *Chaotic communication using generalized synchronization*, Chaos, Solitons & Fractals, vol. 12, pp. 145–152.

Thiffeault, J. & Finn, M. & Gouillart, E. & Hall, T. [2008] *Topology of chaotic mixing patterns*, Chaos: An Interdisciplinary Journal of Nonlinear Science, vol. 18, pp. 33123–33143.

Uchida, A. & Yoshimori, S. & Shinozuka, M. & Ogawa, T. & Kannari, F. [2001] *Chaotic on off keying for secure communications*, Optics letters, vol. 26, pp. 866–868.

Wang, S. & Kuang, J. & Li, J. & Luo, Y. & Lu, H. & Hu, G. [2002] *Chaos-based secure communications in a large community*, Adaptation and Learning in Control and Signal Processing, vol. 66, pp. 065202.

Wang, X. & Gao, Y. [2010] *A switch-modulated method for chaos digital secure communication based on user-defined protocol*, Communications in Nonlinear Science and Numerical Simulation, vol. 15, pp. 99–104.

Xia, X. & Moog, C. [2003] *Identifiability of nonlinear systems with application to HIV/AIDS models*, Automatic Control, IEEE Transactions on, vol. 48, pp. 330–336.

Xiao, Y. & Han, Y. [2007] *An Encrypt Approach Using Dynamic Encrypt keys*, Machine Learning and Cybernetics, 2007 International Conference on, vol. 6, pp. 3273–3277.

& [2013] *Chaotic analog-to-information conversion: principle and reconstructability with parameter identifiability*, International Journal of Bifurcation and Chaos, vol. 23, pp. 1–36.

[2007] *A three-party authenticated key exchange scheme smartcard using elliptic curve cryptosystem for secure key exchange in wireless sensor network*, Consumer Electronics, 2007. ISCE 2007. IEEE International Symposium on, pp. 1–6.

Yang, T. & Yang, L. & Yang, C. [1998] *Breaking chaotic switching using generalized synchronization: Examples*, Circuits and Systems, 1998. ISCAS'98. Proceedings of the 1998 IEEE International Symposium on, vol.45, pp. 1062–1067.

Yang, T. & Yang, L.. & Yang, C. [1998] *Breaking chaotic secure communication using a spectrogram*, Physics Letters A, vol.247, pp. 105–111.

Yang, T. [2004] *A survey of chaotic secure communication systems*, International Journal of Computational Cognition, vol. 2, pp. 81–130.

Zaher, A. & Abu-Rezq, A. [2011] *On the design of chaos-based secure communication systems*, Adaptation , vol. 16, pp. 3721–3737.