International Journal of Bifurcation and Chaos, Vol. 22, No. 9 (2012) 1250231 (11 pages)
© World Scientific Publishing Company
DOI: 10.1142/S0218127412502318

DESYNCHRONIZATION CHAOS SHIFT KEYING METHOD BASED ON THE ERROR SECOND DERIVATIVE AND ITS SECURITY ANALYSIS

SERGEJ ČELIKOVSKÝ* and VOLODYMYR LYNNYK†
Institute of Information Theory and Automation,
Academy of Sciences of the Czech Republic,
P. O. Box 18, Prague 8, 18208, Czech Republic
Department of Control Engineering,
Faculty of Electrical Engineering,
Czech Technical University in Prague, Czech Republic
*celikovs@utia.cas.cz
†volodymyr.lynnyk@utia.cas.cz

Received June 1, 2012

This paper describes the chaos shift keying method based on the second derivative desynchronization error and provides its security analysis, especially against the attacks by power and return map analysis. Desynchronization chaos shift keying method (DECSK) uses methods to detect the correct bit by detecting the wrong bit. Various modifications are possible, here the method using sharp increase of error in the second derivative of synchronizing signal is used. The proposed method requires very reasonable amount of data to encrypt and time to decrypt one bit. Basically, to encrypt one bit, only one iteration (i.e. only one real number of six valid digits) is needed. At the same time, thanks to the desynchronization detection based on the synchronization error second derivative, almost 100% of the carrying chaotic signal can be used. The security of the proposed method can be systematically investigated showing its good resistance against typical decryption attacks. More detailed analysis is devoted to its analysis via power and return map analysis. Conclusion is that the DECSK method cannot be broken by the above two methods which together with other arguments developed there serves as a good basis for the DECSK security.

Keywords: Nonlinear system; desynchronization; chaos shift keying; generalized Lorenz system.

1. Introduction

It is quite well-known fact that many chaotic communication schemes based on chaotic dynamics has been proposed during the past 20 years. As a matter of fact, the well-known features of the chaotic systems like strong dependence on the initial data, topological transitivity, wide spread spectrum of its signal, etc., directly suggest the idea to use suitable chaos generators to build a new generation of secure encryption methods. Nevertheless, methods using continuous time chaos usually consider analogue communication while discrete time chaotic systems are used for digital data encryption. Unfortunately, the use of the continuous time chaotic systems for the encryption of the digital data and both its practical aspects and security analysis have been studied

*Work of this author was supported by the Czech Science Foundation through the research grant no. P103/12/1794.

much less [Alvarez & Li, 2006; Dachselt & Schwarz, 2001; Kocarev, 2001] due to prevalently used analogue chaotic masking [Lian & Liu, 2000; Alvarez-Ramirez *et al.*, 2002]. One of the possible exceptions is the so-called chaos shift keying (CSK) method, which uses time segments of chaotic signals corresponding to two different chaotic systems to encrypt a single bit. Originally, the CSK was introduced (under different name) in [Cuomo *et al.*, 1993] for analogue implementation of the Lorenz system and its synchronized copy and actually again for possible analogue circuit implementation, though meant to encrypt and modulate binary symbols directly into an analogue signal. Therefore, the length of the time segment was not such an issue. Nevertheless, when using computer digital implementation also for chaos generator, such a method is becoming almost ridiculous due to huge amount of data to encrypt a single bit. Moreover, the excessive length of the pieces of signals corresponding to "0" and "1" also enables various statistically based attacks, e.g. the correlation analysis. Summarizing, the classical CSK method leads to weak and slow ciphers.

The first attempt to overcome the above drawbacks was the so-called Desynchronization Chaos Shift Keying (DECSK) method proposed in [Čelikovský *et al.*, 2006a, 2006b], called initially with a slight abuse of notation as the anti-synchronization chaos shift keying method. Desynchronization basically means that, rather than detecting the correct bit via synchronizing one of two unsynchronized slaves, the wrong bit is determined via desynchronizing one of the perfectly synchronized slaves. This method significantly reduced the amount of data needed to encrypt a single bit up to 4–13 iterations. This amount, though no more ridiculous, was still practically useless. Later on, in [Lynnyk & Čelikovský, 2010], thanks to desynchronization detection of the wrong bit based on the error derivative evaluation, the above characteristic has been further reduced up to one iteration per bit. Nevertheless, the desynchronization effect was shown to be dependent on the absolute value of the synchronizing signal, therefore only a smaller percentage of the carrying signal could be used. All the above results were implemented and tested for the so-called Generalized Lorenz System (GLS) [Čelikovský & Vaněček, 1994; Vaněček & Čelikovský, 1996], and [Čelikovský & Chen, 2005] and its special parametrization [Čelikovský & Chen, 2002].

The purpose of this paper is to provide further detailed analysis of the desynchronization estimates of yet another improvement [Čelikovský & Lynnyk, 2009b] of the just mentioned DECSK secure encryption scheme based on the GLS and presented in [Čelikovský *et al.*, 2006a, 2006b; Čelikovský & Lynnyk, 2009a; Lynnyk & Čelikovský, 2010]. This improvement [Čelikovský & Lynnyk, 2009b] consists in keeping the rate of one iteration per bit for about 95% of the carrying chaotic signal. This is made possible thanks to evaluation of the second derivative of the synchronizing error, rather than the first derivative in [Lynnyk & Čelikovský, 2010]. As a matter of fact, while the former reacts on parameter mismatch for small t as $o(1)$, the latter reacts only as $o(t)$. As in [Lynnyk & Čelikovský, 2010], the benefit is taken from the fact that one can easily numerically differentiate signals given digitally with no bias. Therefore, the security analysis of the method from [Čelikovský & Lynnyk, 2009b] is of great interest as well. Such an analysis will be provided based on the power analysis and return map methods. Additional analysis based on the derived desynchronization estimates will be also carried out.

The paper is organized as follows. In the next section, we briefly repeat and complete some known facts about GLS, including the known estimates of the desynchronization effect. Section 3 describes the modification of DECSK method to be analyzed, namely the one based on the detection of the second derivative of the error and provides mathematical analysis of the desynchronization estimates being its basis. Section 4 provides the security analysis of this method against attack using return map [Perez & Cerdeira, 1995; Li *et al.*, 2006] and power analysis methods [Alvarez *et al.*, 2004], as well as its key analysis. The final section gives some conclusions.

2. Generalized Lorenz System, Its Synchronization and Desynchronization

Despite its name, DECSK encryption scheme, introduced later on, relies, similarly as the majority of the chaos based schemes, on the synchronization of two, or more chaotic systems. Therefore, before describing the DECSK scheme, both the synchronization and the desynchronization effects for the GLS system will be studied in detail. More precisely, the estimates for the synchronization level of two GLSs with mismatched parameters will be estimated in this section both from the bottom and the above. First, let us recall some previous results on generalized Lorenz system classification and synchronization. Further details may be found in [Čelikovský & Chen, 2005].

Definition 2.1. The following general nonlinear system of ordinary differential equations in $\mathbb{R}^3$ is called a *Generalized Lorenz System* (GLS):

$$\dot{x} = \begin{bmatrix} A & 0 \\ 0 & \lambda_3 \end{bmatrix} x + \begin{bmatrix} 0 \\ -x_1x_3 \\ x_1x_2 \end{bmatrix}, \quad A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \tag{1}$$

where $x = [x_1 \quad x_2 \quad x_3]^\top$, $\lambda_3 \in \mathbb{R}$, and A has eigenvalues $\lambda_1, \lambda_2 \in \mathbb{R}$, such that

$$-\lambda_2 > \lambda_1 > -\lambda_3 > 0. \tag{2}$$

The inequality (2) goes back to the well-known Shilnikov's chaos analysis near the homoclinicity and can be viewed as the necessary condition for the chaos existence, see more detailed discussion in [Čelikovský & Chen, 2002; Vaněček & Čelikovský, 1996]. GLS is said to be *nontrivial* if it has at least one solution that goes neither to zero nor to infinity nor to a limit cycle. The following result, enabling efficient synthesis of a rich variety of chaotic behaviors for GLS, has been obtained in [Čelikovský & Chen, 2002]:

Theorem 2.2. *For the nontrivial generalized Lorenz system (1)–(2), there exists a nonsingular linear change of coordinates, $z = Tx$, which takes (1) into the following generalized Lorenz canonical form*:

$$\dot{z} = \begin{bmatrix} \lambda_1 & 0 & 0 \\ 0 & \lambda_2 & 0 \\ 0 & 0 & \lambda_3 \end{bmatrix} z + cz \begin{bmatrix} 0 & 0 & -1 \\ 0 & 0 & -1 \\ 1 & \tau & 0 \end{bmatrix} z, \tag{3}$$

where $z = [z_1, z_2, z_3]^\top$, $c = [1, -1, 0]$ and parameter $\tau \in (-1, \infty)$.

Actually, the parameter τ plays an important role of single scalar bifurcation parameter, while remaining parameters only have qualitative influence, being eigenvalues of the approximate linearization of GLS at the origin. These qualitative parameters are just required to satisfy robust condition (2), so that fine tuning may be done using the single scalar parameter τ only.

Synchronization of GLS is based on yet another canonical form, the so-called **observer canonical form of GLS** provided by the following

Theorem 2.3. *Both nontrivial GLS (1) and its canonical form (3) are state equivalent to the following form*:

$$\frac{\mathrm{d}\eta}{\mathrm{d}t} = \begin{bmatrix} (\lambda_1+\lambda_2)\eta_1 + \eta_2 \\ -\eta_1\left[\lambda_1\lambda_2 + (\lambda_1-\lambda_2)\eta_3 + \dfrac{(\tau+1)\eta_1^2}{2}\right] \\ \lambda_3\eta_3 + K_1(\tau)\eta_1^2 \end{bmatrix} \tag{4}$$

$$K_1(\tau) = \frac{\lambda_3(\tau+1) - 2\tau\lambda_1 - 2\lambda_2}{2(\lambda_1-\lambda_2)}, \tag{5}$$

where $\eta = [\eta_1, \eta_2, \eta_3]^\top$, which is referred to in the sequel as the observer canonical form. The corresponding smooth coordinate change and its inverse are

$$\eta = \left[z_1 - z_2, \lambda_1 z_2 - \lambda_2 z_1, z_3 - \frac{(\tau+1)(z_1-z_2)^2}{2(\lambda_1-\lambda_2)}\right]^\top \tag{6}$$

$$z = \left[\frac{\lambda_1\eta_1+\eta_2}{\lambda_1-\lambda_2}, \frac{\lambda_2\eta_1+\eta_2}{\lambda_1-\lambda_2}, \eta_3 + \frac{(\tau+1)\eta_1^2}{2(\lambda_1-\lambda_2)}\right]^\top. \tag{7}$$

Indeed, the above observer canonical form, when viewing $\eta_1 = x_1 = z_1 - z_2$ as the output, is almost in the form linearizable by output injection. This leads to following observer-based synchronization of two copies of GLS.

Theorem 2.4. *Let (2) hold. Consider system (4)–(5), with the output η_1 and its uniformly bounded trajectory $\eta(t)$, $t \geq t_0$. Further, consider the system having input η_1 and the state $\hat{\eta} = (\hat{\eta}_1, \hat{\eta}_2, \hat{\eta}_3)^\top$, being affected by (4)–(5) output η_1 injection as follows*:

$$\frac{\mathrm{d}\hat{\eta}}{\mathrm{d}t} = \begin{bmatrix} l_1 & 1 & 0 \\ l_2 & 0 & 0 \\ 0 & 0 & \lambda_3 \end{bmatrix}\hat{\eta} + \begin{bmatrix} \lambda_1+\lambda_2-l_1 \\ -\lambda_1\lambda_2 - l_2 \\ 0 \end{bmatrix}\eta_1 + \begin{bmatrix} 0 \\ -(\lambda_1-\lambda_2)\eta_1\hat{\eta}_3 - \left(\dfrac{1}{2}\right)(\tau+1)(\eta_1)^3 \\ K_1(\tau)(\eta_1)^2 \end{bmatrix}, \tag{8}$$

where $l_{1,2} < 0$. *Then there exist* $C_1 \geq 1, C_2 > 0$ *such that*

$$\|\eta(t) - \hat{\eta}(t)\| \leq C_1 \exp(-C_2 t)\|\eta(0) - \hat{\eta}(0)\|,$$

i.e. system (8) is a global exponential observer (4)–(5).

Proofs of all previous theorems may be found in [Čelikovský & Chen, 2002]. In the sequel, the system (4)–(5) will be often called as the master while (8) as the slave.

The following two propositions analyze the influence of mismatching the parameter τ in the master and slave, where system (4)–(5) with chaotic behavior is considered. First of them shows upper estimate, i.e. synchronization speed while the second one gives lower estimate, i.e. desynchronization speed.

Proposition 2.5. *Let (2) hold. Consider system (8) with* $\tau = \tau_{sl}(t)$, $l_{1,2} < 0$ *and system (4)–(5) with* $\tau = \tau_{\text{mast}}(t)$, *where* $\tau_{sl}(t)$, $\tau_m(t)$ *are uniformly bounded measurable functions. Further, suppose that for the corresponding state trajectories of (8) and (4)–(5), the Euclidean norm of both* $\eta_1(t)$ *and* $\hat{\eta}_1(t)$ *is uniformly bounded by a constant R. Then, for sufficiently small*

$$\overline{\Theta} := \max_{\tau \in R^+} |\tau_{\text{mast}}(t) - \tau_{sl}(t)|$$

it holds

$$\overline{\lim_{t\to\infty}} \|\eta(t) - \hat{\eta}(t)\| \leq C\overline{\Theta},$$

where $C > 0$ *is a suitable constant. Moreover, for all values of* $l_{1,2}$, *it holds that*

$$\frac{\mathrm{d}(\eta_3 - \hat{\eta}_3)}{\mathrm{d}t} = \lambda_3(\eta_3 - \hat{\eta}_3) + \frac{\lambda_3 - 2\lambda_1}{2(\lambda_1 - \lambda_2)}\Theta(t)\eta_1^2, \qquad (9)$$

$$\Theta(t) := (\tau_{\text{mast}}(t) - \tau_{sl}(t)). \qquad (10)$$

The proof of this proposition and a more specific estimation of the constant C may be found in [Čelikovský *et al.*, 2006b].

Proposition 2.6. *Let (2) hold. Consider system (8) with* $\tau = \tau_{sl}$, $l_{1,2} < -1$ *and system (4)–(5) with* $\tau = \tau_{\text{mast}}$, *where* τ_{sl}, τ_m *are constants. Further, let it hold for some state trajectory* $\eta(t) = [\eta_1(t), \eta_2(t), \eta_3(t)]^\top$ *of (4)–(5)*

$$0 < E < |\eta_1(t)| < R, \quad \forall\, t \in [0, T^*],$$
$$T^* := \min\left(\frac{E^2}{3R^2(2\lambda_1 - \lambda_3)}, \left|\frac{1}{2l_1}\right|, \left|\frac{1}{2l_2}\right|\right).$$

Then it holds for all $t \in [0, T^*]$

$$|\hat{\eta_1}(t) - \eta_1(t)| \geq \frac{E^3}{12}|\Theta|t^2,$$

$$|\hat{\eta_2}(t) - \eta_2(t)| \geq \frac{E^3}{6}|\Theta|t,$$

where $\Theta := \tau_{\text{mast}} - \tau_{sl}$ *and* $\hat{\eta}(t)$ *is any trajectory of (8) with* $\hat{\eta}(0) = \eta(0)$.

The proof of this proposition may be found in [Lynnyk & Čelikovský, 2010].

3. Desynchronization Chaos Shift Keying Scheme Based on the Second Derivative Detection

As already mentioned, to construct our encryption and decryption algorithms, we aim to further improve the DECSK scheme introduced in [Čelikovský *et al.*, 2006a, 2006b] and improved in [Lynnyk & Čelikovský, 2010]. This improvement is based on the following proposition.

Proposition 3.1. *Let (2) hold. Consider system (8) with* $\tau = \tau_{sl}$, $l_1 < l_2 \leq -1$ *and system (4)–(5) with* $\tau = \tau_{\text{mast}}$, *where* τ_{sl}, τ_m *are constants. Further, let it hold for some state trajectory* $\eta(t) = [\eta_1(t), \eta_2(t), \eta_3(t)]^\top$ *of (4)–(5) that*

$$0 < E < |\eta_1(t)| < R, \quad \forall\, t \in [0, T^*],$$
$$T^* := \min\left(\frac{1}{2\lambda_1 - \lambda_3}, \left|\frac{1}{2l_1}\right|, \left|\frac{1}{2l_2}\right|\right).$$

Then it holds for all $t \in [0, T^*]$

$$|\ddot{e}_1(t)| \geq \frac{|\Theta|}{2}\left[E^3 - R^3\left[2(l_1^2 + l_2)t^2 + (2\lambda_1 - \lambda_3 - 4l_1)t\right]\right]$$

where $\Theta := \tau_{\mathrm{mast}} - \tau_{sl}$, $e_1(t) := \hat{\eta}_1(t) - \eta_1(t)$ *and* $\hat{\eta}(t)$ *is any trajectory of* (8) *with* $\hat{\eta}(0) = \eta(0)$.

Proof. Obviously, the following error dynamics holds:

$$\dot{e} = \begin{bmatrix} l_1 & 1 & 0 \\ l_2 & 0 & (\lambda_2 - \lambda_1)\eta_1 \\ 0 & 0 & \lambda_3 \end{bmatrix} e + \begin{bmatrix} 0 \\ \dfrac{\Theta\eta_1^3}{2} \\ -\dfrac{\lambda_3 - 2\lambda_1}{2(\lambda_1 - \lambda_2)}\Theta\eta_1^2 \end{bmatrix},$$

where $e(t) :\equiv \hat{\eta}(t) - \eta(t)$. Recall that by the assumption of the proposition being proved, we get $e(0) = \hat{\eta}(0) - \eta(0) = 0$. Then

$$e_3(t) = \frac{\lambda_3 - 2\lambda_1}{2(\lambda_1 - \lambda_2)}\Theta \int_0^t \exp(\lambda_3(t-s))\eta_1^2(s)\mathrm{d}s,$$

Recall, that $\lambda_2 < 0, \lambda_3 < 0, \lambda_1 > 0$, therefore it holds

$$|e_3(t)| = \frac{2\lambda_1 - \lambda_3}{2(\lambda_1 - \lambda_2)}|\Theta| \int_0^t \exp(\lambda_3(t-s))\eta_1^2(s)\mathrm{d}s,$$

and by virtue of the assumption $|\eta_1(t)| < R$, $\forall\, t \in [0, T^*]$

$$|e_3(t)| \le \frac{2\lambda_1 - \lambda_3}{2(\lambda_1 - \lambda_2)}|\Theta|R^2 \int_0^t \exp(\lambda_3(t-s))\mathrm{d}s$$
$$\le \frac{2\lambda_1 - \lambda_3}{2(\lambda_1 - \lambda_2)}|\Theta|R^2 t.$$

Further, let

$$\tilde{A} = \begin{bmatrix} l_1 & 1 \\ l_2 & 0 \end{bmatrix}, \tag{11}$$

then

$$\begin{bmatrix} e_1(t) \\ e_2(t) \end{bmatrix} = \int_0^t \exp(\tilde{A}(t-s)) \begin{bmatrix} 0 \\ \alpha(s) \end{bmatrix} \mathrm{d}s, \quad \alpha(s) = (\lambda_2 - \lambda_1)\eta_1(s)e_3(s) - \frac{\Theta\eta_1^3(s)}{2},$$

$$|\alpha(s)| = \left|(\lambda_2 - \lambda_1)e_3(s) - \frac{\Theta\eta_1^2(s)}{2}\right| |\eta_1(s)| \le \frac{|\Theta|R^3}{2} + |(\lambda_1 - \lambda_2)e_3(s)|R \le R^3|\Theta|\frac{1 + (2\lambda_1 - \lambda_3)s}{2},$$

i.e.

$$|\alpha(s)| \le |\Theta|R^3, \quad \forall\, s \in [0, (2\lambda_1 - \lambda_3)^{-1}],$$

$$e_1(t) = \int_0^t \alpha(t-s)\left[s + \frac{l_1 s^2}{2} + \frac{(l_1^2 + l_2)s^3}{6} + \cdots\right]\mathrm{d}s, \quad e_2(t) = \int_0^t \alpha(t-s)\left[1 + \frac{l_2 s^2}{2} + \frac{(l_1 l_2)s^3}{6} + \cdots\right]\mathrm{d}s,$$

$$|e_1(t)| = |\Theta|R^3\left[\frac{t^2}{2} + \frac{l_1 t^3}{6} + \frac{(l_1^2 + l_2)t^4}{24} + \cdots\right]\mathrm{d}s \le \frac{1}{2}|\Theta|R^3 t^2\left[1 + \frac{l_1 t}{6} + \frac{(l_1^2 + l_2)t^2}{24} + \cdots\right] \le |\Theta|R^3 t^2,$$

$$|e_2(t)| = |\Theta|R^3\left[t + \frac{l_1 t^3}{6} + \frac{(l_1 l_2)t^4}{24} + \cdots\right]\mathrm{d}s \le |\Theta|R^3 t\left[1 + \frac{l_2 t^2}{6} + \frac{(l_1 l_2)t^3}{24} + \cdots\right]$$
$$\le 2|\Theta|R^3 t, \quad t \in [0, T^*], \quad T^* := \min\left[(2\lambda_1 - \lambda_3)^{-1}, \frac{-1}{l_1}, \frac{-1}{l_2}\right].$$

In other words, it holds

$$|e_1(t)| \le R^3|\Theta|t^2, \quad |e_2(t)| \le 2R^3|\Theta|t, \quad \forall\, t \in [0, T^*].$$

Now, using the derived upper estimates of $|e_{1,2,3}(t)|$ and both the lower and upper estimates of $|\eta_1(t)|$, assumed in the proposition statement, one can finish this proof as follows

$$\ddot{e}_1 = l_1\dot{e}_1 + \dot{e}_2$$
$$= (l_1^2 + l_2)e_1 + l_1 e_2 + (\lambda_2 - \lambda_1)\eta_1(t)e_3(t) - \frac{\Theta\eta_1^3(t)}{2},$$

$$|\ddot{e}_1(t)| \ge \left|\frac{\Theta\eta_1^3(t)}{2}\right| - |(l_1^2 + l_2)e_1 + l_1 e_2 + (\lambda_2 - \lambda_1)\eta_1(t)e_3(t)|.$$

Therefore, taking into the account all those previously derived estimates of $e_{1,2,3}(t)$ $\forall\, t \in [0, T^*]$ and

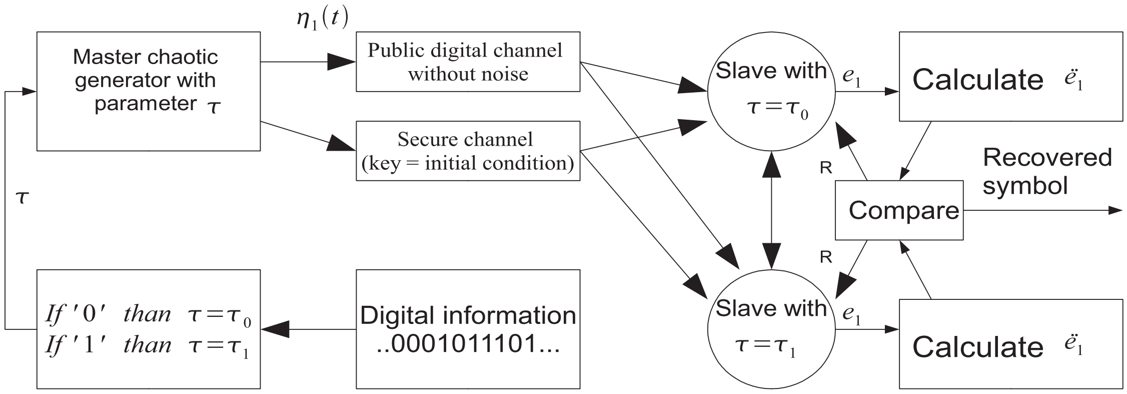

$\eta_1(t)$
Master chaotic generator with parameter τ
Public digital channel without noise
Secure channel (key = initial condition)
τ
If '0' than $\tau=\tau_0$
If '1' than $\tau=\tau_1$
Digital information ..0001011101...
Slave with $\tau=\tau_0$
Slave with $\tau=\tau_1$
e_1
e_1
R
R
Calculate $\ddot{e}_1$
Calculate $\ddot{e}_1$
Compare
Recovered symbol

Fig. 1. DECSK digital communication system with desynchronization-error-based demodulator.

$l_1 \le l_2 \le -1$, $-\lambda_2 > \lambda_1 > -\lambda_3 > 0$ from the proposition assumption, we get

$$|\ddot{e}_1(t)| \ge \frac{|\Theta|E^3}{2} - (l_1^2 + l_2)R^3|\Theta|t^2 + 2l_1R^3|\Theta|t - (\lambda_2 - \lambda_1)R\frac{2\lambda_1 - \lambda_3}{2(\lambda_1 - \lambda_2)}|\Theta|R^2t,$$

$$|\ddot{e}_1(t)| \ge \frac{|\Theta|}{2}\big[E^3 - R^3\big[2(l_1^2 + l_2)t^2 + (2\lambda_1 - \lambda_3 - 4l_1)t\big]\big],$$

which completes the proof. ■

Remark 3.2. Typical length of the single iteration used during desynchronization detection is 0.001. Therefore, practically, the desynchronization speed of the second derivative of the synchronizing signal error may be taken as

$$|\ddot{e}_1(t)| \ge \frac{|\Theta|E^3}{2}. \tag{12}$$

As a matter of fact, during this very short time interval, one can assume that $R/E \approx 1$ (i.e. minimum and maximum values of synchronizing signal are practically the same). Therefore, the claim of the current remark follows from the fact that

$$1 - 2(l_1^2 + l_2)t^2 - (2\lambda_1 - \lambda_3 - 4l_1)t \approx 1 \quad \text{for } t = 0.001.$$

One can therefore see that DECSK based on the second derivative detection has much better potential for the encryption. This scheme is clearly described in Fig. 1.

On the transmitter side, there is the signal generator being the GLS (4)–(5) depending on crucial bifurcation parameter τ [Čelikovský & Chen, 2002; Čelikovský & Vaněček, 1994; Vaněček & Čelikovský, 1996]. To encrypt digital information, one chooses "for a while" $\tau = \tau_0$ for bit "0" while for the bit "1" one chooses $\tau = \tau_1$, where τ_0, τ_1 are suitably selected GLS bifurcation parameters from its known chaotic range, cf. [Čelikovský & Chen, 2002; Čelikovský & Vaněček, 1994; Vaněček & Čelikovský, 1996; Čelikovský & Chen, 2005]. Then, only the first component of a chaotic signal $\eta_1 = x_1 = z_1 - z_2$ will be transmitted through the communication channel.

On the receiver side, signal $\eta_1 = x_1 = z_1 - z_2$ is fed into two synchronized copies of GLS (the so-called slaves), the first one, with parameter τ_0, while the second one with parameter τ_1. Now, the crucial idea of **desynchronization** based decryption uses the fact that both slaves are kept synchronized to the numerically best possible level (the so-called **numerical zero**, in most simulations[1] equal to 10^{-4}). Therefore, one can detect almost immediately "the wrong" slave due to the fact that it produces fast increasing error of its first component compared to the slowly varying error in "the correct" slave. In such a way, the bit value is decrypted, moreover, the state value of the "wrong" slave is overwritten by the value from the "correct" slave, so that prior to receiving the next piece of cipher text (i.e. the synchronizing signal $\eta_1(t)$) both slaves are again synchronized to the same best possible level of the "numerical zero" 10^{-4}.

This idea was developed in [Čelikovský *et al.*, 2006b, 2006a] by comparing error values $e_1(t) = \eta_1 - \hat{\eta}_1$ in both slaves. The drawback was need for more iterations to wait for sufficiently safe large

[1] MATLAB-SIMULINK ode4 Runge–Kutta procedure with a fixed step size 0.001 is being used throughout the paper.

Table 1. Here, $P(E) = \frac{\text{meas}(A(E))}{T_{\max}} \cdot 100$, where $A(E) = \{t \in [0, T_{\max}] : |\eta_1(t)| \geq E\}$ and $T_{\max}$ is maximal time available during simulation.

E	4.0	3.0	2.0	1.5	1	0.8	0.6	0.5	0.4	0.3	0.25	0.1
P(E)	19.92	28.14	38.18	47.51	64.76	71.45	78.32	81.25	84.44	87.44	89.08	95.07

error. Typically, (∼4–13) iterations were needed, moreover, only a small percentage of signal carrier could be used. Later on, in [Lynnyk & Čelikovský, 2010], the method was improved by considering the second component detection.

The current method uses Proposition 3.1 and computes numerically the second derivative $\ddot{e}_1$ in both slaves. As expected by Proposition 3.1 and confirmed by the simulations presented in detail later on, it is possible to detect the wrong slave immediately for the higher percentage of synchronizing signal — being, in fact, the cipher text carrier.

As a matter of fact, as shown by all Propositions 2.5, 2.6, 3.1, for the fixed parameter mismatch $\Theta = |\tau_{\text{mast}} - \tau_{sl}|$ the desynchronization effect crucially depends on the absolute value of the synchronizing signal η_1, namely, on E^3, where E is minimal value of $\eta_1(t)$ over the time interval where desynchronization is to be detected. This crucial value has been experimentally analyzed thoroughly and their percentual summary is given in Table 1.

To demonstrate a huge progress made by the current approach, consider Table 1. DECSK method of [Čelikovský *et al.*, 2006a, 2006b] needed $E \geq 4$ to detect binary signals after 13 iterations (i.e. ≈20% of signal carrier could be used), DECSK presented in [Lynnyk & Čelikovský, 2010] requires single iteration provided $E \geq 2$. The current method requires single iteration for $E \geq 0.33$ (i.e. for 86.44% of signal carrier), and two iterations for $E \geq 0.1$ (95.07%). Summarizing, the current method can encrypt/decrypt efficiently 920 bits/1000 iterations, comparing to just 15 bits/1000 iterations for the very first method in [Čelikovský *et al.*, 2006a, 2006b] and 370 bits/1000 iterations for the method in [Lynnyk & Čelikovský, 2010].

Example of the application of the current DECSK method is shown in Fig. 2. It shows an example of a transmitted baseband signal for the message "0001011101" encoded by means of two different, but close to each other chaotic GLS generators with different parameters $\tau_0 = 0.1$ and $\tau_1 = 0.2$. Only the ciphertext is available to potential intruder with no clue of encrypted signal. This ciphertext is the synchronizing signal sent by either GLS with $\tau_0 = 0.1$ or $\tau_1 = 0.2$, depending on an encrypted value of the current bit. For easy mutual comparison of all scopes in Fig. 2, their time axes are identical and indicates number of iterations, not a real time. Here, one can clearly see the influence of parameter mismatch on the second derivative (see the second graph from the bottom), easily detectable even by single iteration, while comparison of the errors only (see the middle graph) by no means may detect the correct value.

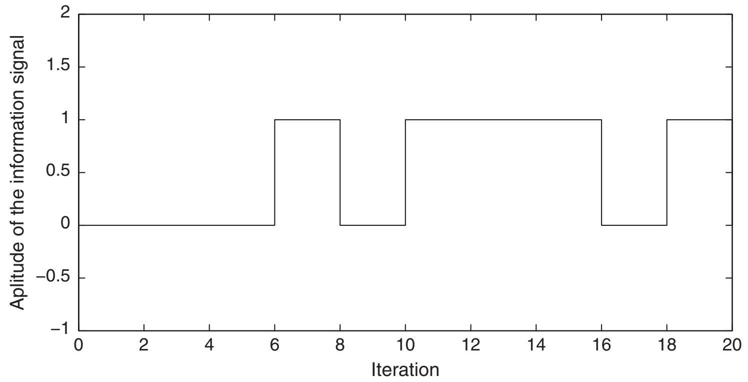


Fig. 2. Time histories related with the encryption and decryption of the plaintext "0001011101" using DECSK method. From up to down: plaintext time signal; ciphertext; $e_1(t)$; $\ddot{e_1}(t)$ and the reconstructed plaintext.

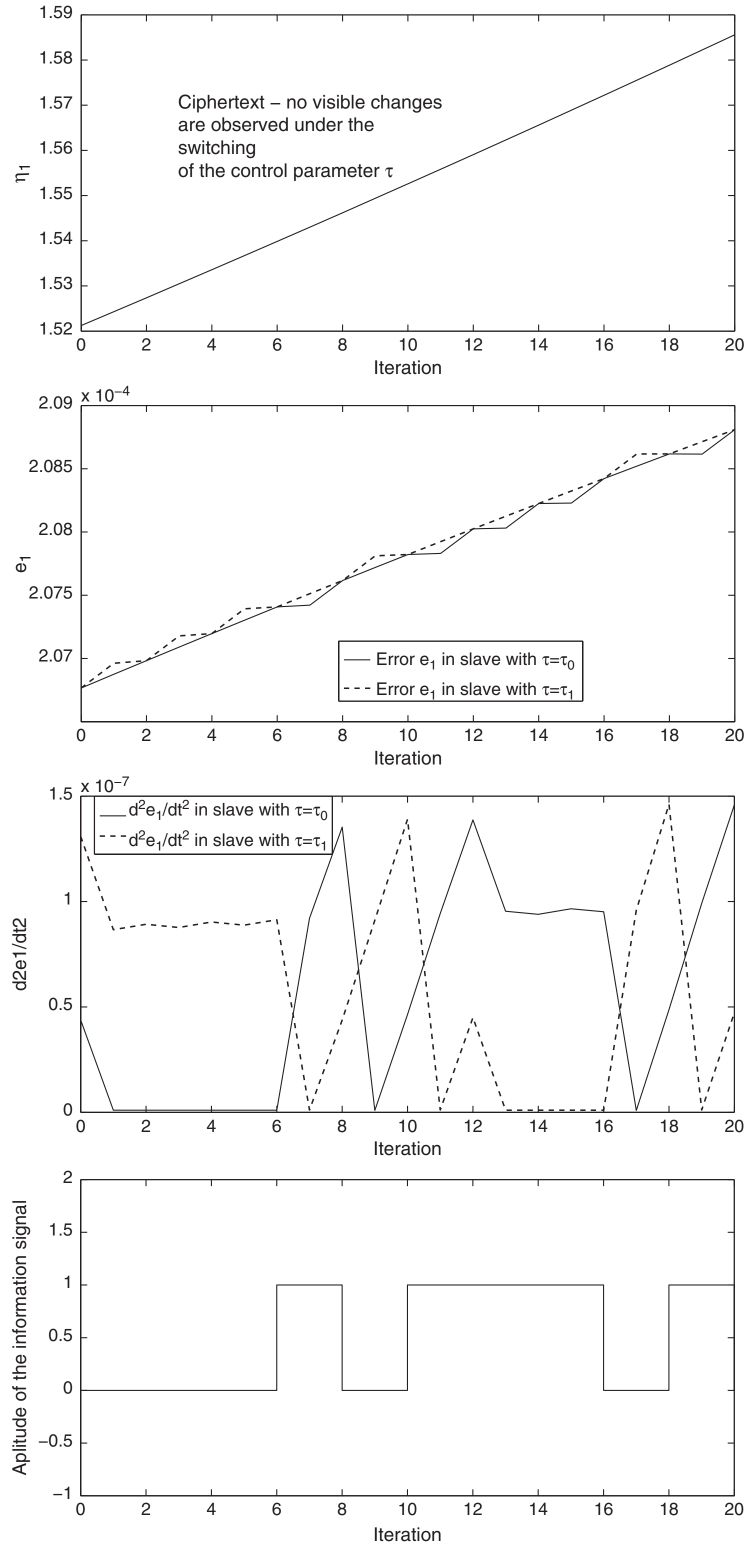


Fig. 2. (*Continued*)

Finally, notice that previously presented Chaos Shift Keying method [Parlitz *et al.*, 1992; Dedieu *et al.*, 1993] typically needs up to a second piece of synchronizing signal to encrypt and decrypt a single bit which corresponds usually to thousands of real numbers (iterations). So, the message expansion and speed of encryption–decryption for CSK method are simply unrealistic. For our DECSK, the message expansion is still much bigger than in methods based on discrete time chaos, nevertheless, it is becoming realistic and might be justified if it provides some extra security.

4. Security Analysis of DECSK Method

4.1. *Power analysis attack*

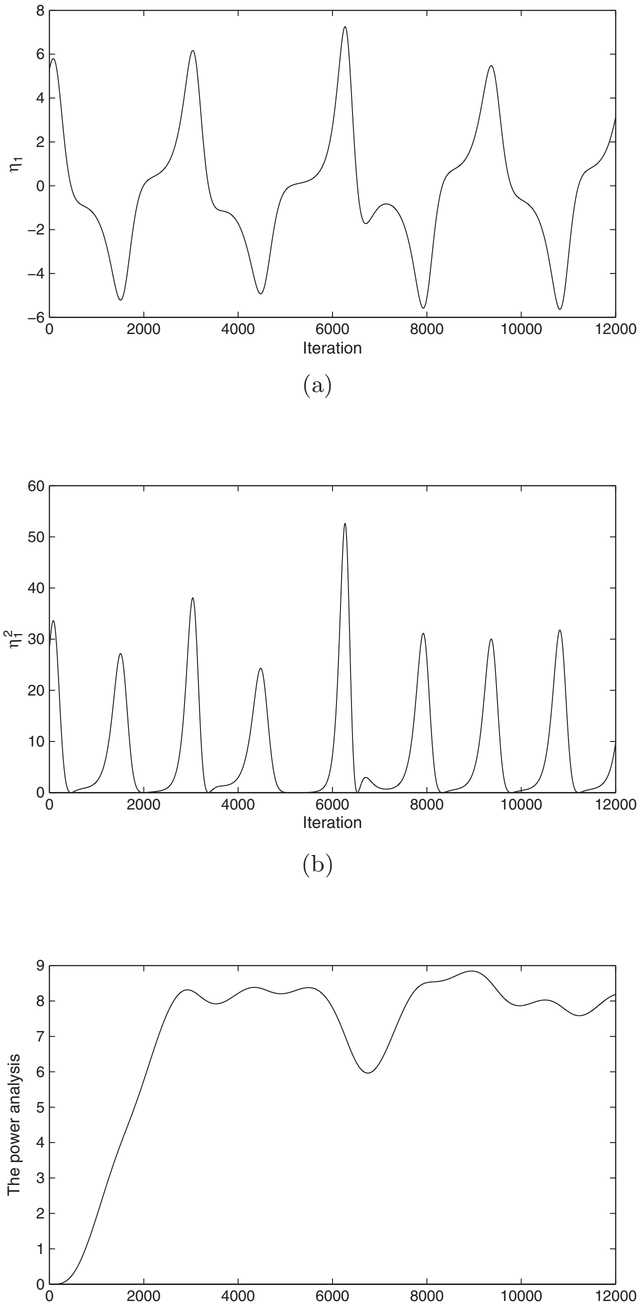
First, to investigate the security of the DECSK scheme, the famous power analysis attack proposed in [Alvarez *et al.*, 2004] is considered. The procedure to analyze the ciphertext of chaos-based security communication scheme proposed there is as follows. Figure 3 plots the result of power analysis attack against DECSK scheme. This attack at first computes the square of the ciphertext signal (the transmitted signal) η_1. Next, this signal η_1^2 is filtered by a low-pass filter, and then the plaintext is recovered using a binary quantizer. Figure 3 plots the result of the power analysis attack for DECSK scheme. From Fig. 3(c) it is obvious that the intruder cannot recover the binary sequence as the signal energy is not changed depending on "0" or "1" being encrypted. Actually, signal in Fig. 3 represents about 12 000 bits (one bit per iteration), and change of energy is affected only globally, by carrying signal time change, not by bits being encrypted.

4.2. *Return map attack*

As described in [Perez & Cerdeira, 1995], a small change of the parameters of the transmitter affects the attractor of the chaotic system. Assuming that X_n and Y_n are the nth maxima and n-minima of the transmitted signal, respectively, define the following modified return maps by $A_n = \frac{X_n+Y_n}{2}$, and $B_n = X_n - Y_n$. In Fig. 4, the plot of the return map limit attractor shows that there are no clear attractor clusters corresponding to different values of parameter τ. Again, the reasons are expectable by the fact that values of τ_0 and τ_1 are close to each other and that changes are made usually each iteration, so that there is actually no two separate attractors. Therefore, the intruder cannot decrypt the plaintext by return map analysis.

4.3. *Key analysis*

The above described decryption scheme in the DECSK method requires initial synchronization of the master on the transmitter side and both slaves on the receiver side, up to the best available numerical precision, called in the sequel as the "numerical zero". Therefore, the initial condition is the immediate candidate for the secret key. As our "numerical zero" is 10^{-4}, this key space is naturally discretized



(a)

(b)

(c)

Fig. 3. Time histories related with the decryption of the plaintext "001101110001000111000110110O" repeated 400 times using power analysis attack. From up to down: (a) the ciphertext, η_1; (b) squared ciphertext signal, η_1^2; (c) low pass filtered squared ciphertext signal.

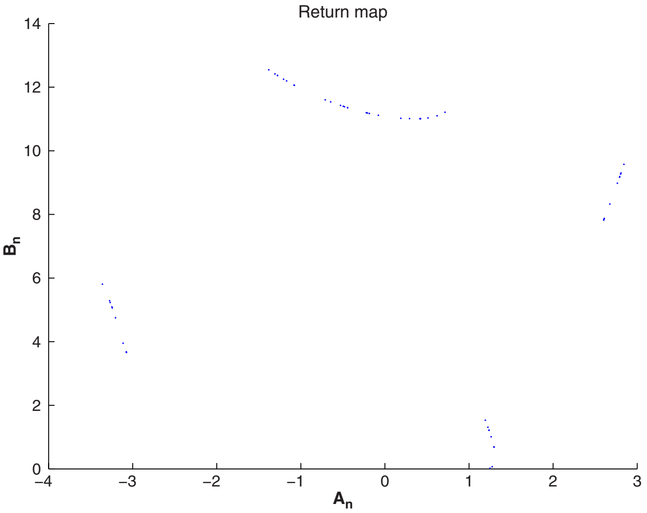


Fig. 4. Return map analysis of DECSK scheme.

in the sense that two initial conditions closer to each other than numerical zero should be represented by the same key. Assuming the size of the initial conditions interval of $\eta_3(t)$ being 10 gives 10^5 different keys, as only the third component $\eta_3(t)$ is unknown, while the first one $\eta_1(t)$ is transmitted through the public channel and the second one $\eta_2(t)$ is easily obtained from the first component $\eta_1(t)$ using the first equation in (4).

To analyze the security of the key based on the initial condition, assume for simplicity at first that both τ_0 and τ_1 are publicly known. Proposition 2.5 implies that at least ten thousands of iterations of the correct signal are needed to synchronize the slaves if the initial conditions of the master are unknown. Therefore, the initial condition key can be broken only in three ways:

- Attack based on the **known** plaintext and the corresponding ciphertext, but both should be at least as of 10 000 bits. Moreover, such a knowledge should be used only for the attack to decrypt some unknown ciphertext **following right after** the above known sequence of both plaintext and the corresponding ciphertext.
- Trying $2^{10\,000}$ possible combinations of all 10 000 bits long plaintexts and comparing them with ciphertext at hand.
- Trying all possible keys — 10^5 initial conditions.

Furthermore, the parameters τ_0, τ_1 can be considered as an additional source for the secret keys. In this case, the current method presents important improvement due to the fact that changes of the parameter may occur during a single iteration. Therefore, one cannot see any clue of changing parameter when analyzing signal η_1. Nevertheless, the difference $|\tau_0 - \tau_1|$ cannot be arbitrarily small, as the desynchronization effect depends on this difference as well, see Propositions 2.5, 2.6, 3.1. Still, this difference was experimentally shown to be possible up to 10^{-3}. Therefore, there are 10^6 possibilities, if values $\tau \in [-0.5, 0.5]$ are considered. As a matter of fact, chaotic range for τ is even broader that the previous interval, see [Čelikovský, 2004]. Finally, notice that secret key based on parameter τ is equally resistant even in the case of the known plaintext and the corresponding sequence of ciphertext. In all kinds of attacks, one has to check all 10^6 possibilities of pairs τ_0, τ_1 and one needs to know the initial condition, treated before.

Therefore, combining both the initial condition and parameter τ, one has up to 10^{11} possibilities for the secret key. When checking all possibilities for the secret key trying to perform the brute force attack, one has to take into the account that the amount of computing efforts to be done for each key choice is far from being negligible. Basically, one needs to evaluate error in both slaves during several iterations and compute its second derivative to see if it stays significantly smaller in one of the slaves than in the other. This leads to a conclusion that brute force attack is unrealistic as well.

Here, an independent use of the τ based key and the initial condition $\eta_3(0)$ based key is guaranteed by the estimates in Proposition 3.1. Indeed, τ mismatch level Θ and initial error $e_3(0)$ influence are mixed on the right-hand side, and nonzero value of any of them spoils a possible detection.

5. Conclusion

Desynchronization estimates for yet another modification of the DECSK scheme has been derived and further security analysis provided. This method is based on the evaluation of the second derivative of the error, which is numerically possible for digital implementations where no noise is present. The security has been analyzed using return map and power analysis method, moreover, desynchronization estimates has been used for the security analysis of possible secret keys.

References

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

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

Alvarez-Ramirez, J., Puebla, H. & Cervantes, I. [2002] "Stability of observer-based chaotic communications for a class of Lur'e systems." *Int. J. Bifurcation and Chaos* **12**, 1605–1618.

Čelikovský, S. & Vaněček, A. [1994] "Bilinear systems and chaos," *Kybernetika* **30**, 403–424.

Čelikovský, S. & Chen, G. [2002] "On a generalized Lorenz canonical form of chaotic systems," *Int. J. Bifurcation and Chaos* **12**, 1789–1812.

Čelikovský, S. [2004] "Observer form of the hyperbolic-type generalized Lorenz system and its use for chaos synchronization," *Kybernetika* **40**, 649–664.

Čelikovský, S. & Chen, G. [2005] "Secure synchronization of a class of chaotic systems from a nonlinear observer approach," *IEEE Trans. Automat. Contr.* **50**, 76–82.

Čelikovský, S., Lynnyk, V. & Šebek, M. [2006a] "Anti-synchronization chaos shift keying method based on generalized Lorenz system," *Proc. 1st IFAC Conf. Analysis and Control of Chaotic Systems*, pp. 333–338.

Čelikovský, S., Lynnyk, V. & Šebek, M. [2006b] "Observer-based chaos sychronization in the generalized chaotic Lorenz systems and its application to secure encryption," *Proc. 45th IEEE Conf. Decision and Control*, pp. 3783–3788.

Čelikovský, S. & Lynnyk, V. [2009a] "Anti-synchronization chaos shift keying method: Error derivative detection improvement," *Proc. 2nd IFAC Conf. Analysis and Control of Chaotic Systems*, pp. 1–6.

Čelikovský, S. & Lynnyk, V. [2009b] "Efficient chaos shift keying method based on the second error derivative anti-synchronization detection," *Proc. 7th IEEE Int. Conf. Control and Automation*, pp. 530–535.

Cuomo, K., Oppenheim, A. & Strogatz, S. [1993] "Synchronization of Lorenz-based chaotic circuits with applications to communications," *IEEE Trans. Circuits Syst.-II: Anal. Dig. Sign. Process.* **40**, 626–633.

Dachselt, F. & Schwarz, W. [2001] "Chaos and cryptography," *IEEE Trans. Circuits Syst.-I: Fund. Th. Appl.* **48**, 1498–1509.

Dedieu, H., Kennedy, M. P. & Hasler, M. [1993] "Chaos shift keying: Modulation and demodulation of a chaotic carrier using self-synchronizing Chua's circuit," *IEEE Trans. Circuits Syst.-II* **40**, 634–642.

Kocarev, L. [2001] "Chaos-based cryptography: A brief overview," *IEEE Circuits Syst. Mag.* **1**, 6–21.

Li, S., Chen, G. & Álvarez, G. [2006] "Return-map cryptoanalysis revisited," *Int. J. Bifurcation and Chaos* **16**, 1157–1168.

Lian, K.-Y. & Liu, P. [2000] "Synchronization with message embedded for generalized Lorenz chaotic circuits and its error analysis," *IEEE Trans. Circuits Syst.-I: Fund. Th. Appl.* **47**, 1418–1424.

Lynnyk, V. & Čelikovský, S. [2010] "Anti-synchronization chaos shift keying method based on generalized Lorenz system," *Kybernetika* **46**, 1–18.

Parlitz, U., Chua, L. O., Kocarev, L., Halle, K. S. & Shang, A. [1992] "Transmission of digital signals by chaotic synchronization," *Int. J. Bifurcation and Chaos* **2**, 973–977.

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

Vaněček, A. & Čelikovský, S. [1996] *Control Systems: From Linear Analysis to Synthesis of Chaos* (Prentice-Hall, London).