Volodymyr Lynnyk; Sergej Čelikovský

On the anti–synchronization detection for the generalized Lorenz system and its applications to secure encryption

Kybernetika, Vol. 46 (2010), No. 1, 1--18

Persistent URL: http://dml.cz/dmlcz/140049

KYBERNETIKA — VOLUME *46* (2010), NUMBER 1, PAGES 1–18

ON THE ANTI–SYNCHRONIZATION DETECTION FOR THE GENERALIZED LORENZ SYSTEM AND ITS APPLICATIONS TO SECURE ENCRYPTION

Volodymyr Lynnyk and Sergej Čelikovský

In this paper, a modified version of the Chaos Shift Keying (CSK) scheme for secure encryption and decryption of data will be discussed. The classical CSK method determines the correct value of binary signal through checking which initially unsynchronized system is getting synchronized. On the contrary, the new anti-synchronization CSK (ACSK) scheme determines the wrong value of binary signal through checking which already synchronized system is loosing synchronization. The ACSK scheme is implemented and tested using the so-called *generalized Lorenz system* (GLS) family making advantage of its special parametrization. Such an implementation relies on the parameter dependent synchronization of several identical copies of the GLS obtained through the observer-based design for nonlinear systems. The purpose of this paper is to study and compare two different methods for the anti-synchronization detection, including further underlying theoretical study of the GLS. Resulting encryption schemes are also compared and analyzed with respect to both the encryption redundancy and the encryption security. Numerical experiments illustrate the results.

Keywords: nonlinear system, observer, chaos shift keying, generalized Lorenz system, synchronization, anti-synchronization, secure communication

Classification: 93C10, 37N25

1. INTRODUCTION AND PROBLEM STATEMENT

A large number of communication schemes that are based on chaos synchronization have been proposed during the last decades [3, 11, 15, 16, 17, 21, 25]. The key idea is very simple and attractive: thanks to the well-known features of the chaotic systems like strong dependence on initial data, topological transitivity, wide spread spectrum of its signal, there is a great potential for hiding sensitive information. Unfortunately, both practical aspects and security analysis are studied much less [2, 13, 18, 23], especially for continuous time systems due to prevalently used chaotic masking [1, 20]. Moreover, to encrypt the digital data, so desirable for prominent internet applications, currently, almost only discrete time chaotic systems are used. One of the possible exceptions is the so-called *Chaos Shift Keying (CSK)* secure encryption scheme, applicable to continuous time systems as well [14, 22]. The CSK method 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 [11, 12] for analogue implementation of the Lorenz system and its synchronized copy. Therefore, the length of the time segment was not such an issue. Nevertheless, when using computer digital implementation, 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. As a typical, and unfortunately very fresh example, see [19], where an unrealistic encryption/decryption scheme was presented without any glimpse of security analysis. Each bit is represented by segment of trajectory of length 1500, so the correlation analysis would easily reveal switching of chaotic generators. Despite a questionable security, to encrypt 1 bit, about 1.5×10^7 iterations are needed. Each iteration is represented by a real number of high precision, so amount of data to encrypt a single bit is useless for the digital data transmission.

The purpose of this paper is to analyze the so-called anti-synchronization effect in the synchronized chaotic systems and to use it for the realistic encryption/decryption schemes design. More precisely, when the synchronization scheme depends on the precise knowledge of some crucial system parameter, its mismatch causes the immediate lost of synchronization. Recently, this effect has been used to design the novel modification the CSK secure encryption scheme, the so-called *anti-synchronization chaos shift keying method (ACSK)*, [7, 8, 9]. As a pilot system for testing the ACSK, the generalized Lorenz system (GLS) [6, 10, 24] and its special parametrization [5] has been used. The ACSK scheme uses the effect of the anti-synchronization, rather than synchronization. More specifically, the classical CSK method determines the correct value of binary signal through checking which unsynchronized system is getting synchronized. On the contrary, the ACSK scheme determines the *wrong* value of binary signal through checking which already synchronized system is loosing synchronization. The advantage of the proposed method is two-fold. First, it requires a very reasonable amount of data to encrypt and time to decrypt a single bit. Secondly, its security can be investigated and estimated as practically unbreakable. The main reason for both advantages is that anti-synchronization is usually thousands times faster than synchronization, even when using two close each to other chaotic systems. Use of close each to other chaotic systems is enabled by mentioned special parametrization of GLS and it is further very important aspect of the security, in particular, making the successful correlation analysis extremely unlikely.

In the present paper, all these advantages will be theoretically justified as well as thoroughly quantitatively tested for GLS through numerical experiments. The ACSK scheme heavily depends on the ability to reveal quickly the parameter mismatch via anti-synchronization detection. Therefore, two methods for the anti-synchronization detection will be suggested and compared. Subsequently, the resulting two ACSK encryption scheme versions will be described and analyzed both on their efficiency and security.

The paper is organized as follows. The next section analyzes mathematically the synchronization and anti-synchronization properties of the generalized Lorenz

system which constitutes the main theoretical contribution of the paper. Section 3 describes two versions of the ACSK method which are illustrated by numerical experiments described in Section 4. Redundancy and security analysis of both ACSK versions is given in Section 5. Final section gives some conclusion and outlooks for further research.

2. SYNCHRONIZATION AND ANTI–SYNCHRONIZATION MEASURE OF THE GENERALIZED LORENZ SYSTEM

This section presents the main theoretical contribution of the paper being the analysis of properties of the special class of ODE – the so-called generalized Lorenz system (GLS). Namely, both the synchronization and the anti-synchronization effects for the GLS system will be studied in detail. In particular, the estimates for the synchronization level of two GLS's with mismatched parameters will be obtained in this section. These estimates will be shown to be valid even in the case when, with slight abuse of terminology, parameters are time-varying. On the other hand, the estimates how quickly initially mutually perfectly synchronized systems reach such an error level will be derived as well.

2.1. Generalized Lorenz system and its synchronization

First, let us recall some previously published results on generalized Lorenz system classification and synchronization. Further details may be found in [6, 7, 9, 8].

Definition 1. The following general nonlinear system of ordinary differential equations in $\mathbb{R}^3$ is called a *generalized Lorenz system* (GLS):

$$\dot{x} = \begin{bmatrix} A & 0 \\ 0 & \lambda_3 \end{bmatrix} x + \begin{bmatrix} 0 \\ -x_1 x_3 \\ x_1 x_2 \end{bmatrix}, \qquad A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \tag{1}$$

where $x = [x_1 \;\; x_2 \;\; x_3]^\top$, $\lambda_3 \in \mathbb{R}$, 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 [5, 24]. 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 the efficient synthesis of a rich variety of chaotic behaviors for GLS, has been obtained in [5].

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

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

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

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

$$\eta = \begin{bmatrix} z_1 - z_2, & \lambda_1 z_2 - \lambda_2 z_1, & z_3 - \frac{(\tau+1)(z_1-z_2)^2}{2(\lambda_1-\lambda_2)} \end{bmatrix}^\top, \tag{6}$$

$$z = \begin{bmatrix} \frac{\lambda_1\eta_1+\eta_2}{\lambda_1-\lambda_2}, & \frac{\lambda_2\eta_1+\eta_2}{\lambda_1-\lambda_2}, & \eta_3 + \frac{(\tau+1)\eta_1^2}{2(\lambda_1-\lambda_2)} \end{bmatrix}^\top. \tag{7}$$

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 the following observer-based synchronization of two copies of GLS.

Theorem 4. Consider system (4) – (5) with the output η_1 and its uniformly bounded trajectory $\eta(t)$, $t \geq t_0$. Further, consider the following system having input η_1^m and state $\hat{\eta} = (\hat{\eta}_1, \hat{\eta}_2, \hat{\eta}_3)^\top$:

$$\frac{\mathrm{d}\hat{\eta}}{\mathrm{d}t} = \begin{bmatrix} l_1 & 1 & 0 \\ l_2 & 0 & 0 \\ 0 & 0 & \lambda_3 \end{bmatrix} \hat{\eta} + \begin{bmatrix} \lambda_1 + \lambda_2 - l_1 \\ -\lambda_1\lambda_2 - l_2 \\ 0 \end{bmatrix} \eta_1^m$$

$$+\begin{bmatrix} 0 \\ -(\lambda_1-\lambda_2)\eta_1^m\hat{\eta}_3-(1/2)(\tau+1)(\eta_1^m)^3 \\ K_1(\tau)(\eta_1^m)^2 \end{bmatrix}, \tag{8}$$

where $l_{1,2}<0$. For all $\varepsilon\geq 0$, assume $|\eta_1(t)-\eta_1^m(t)|\leq\varepsilon$. Then, it holds exponentially in time that

$$\overline{\lim}_{t\to\infty}\|\eta(t)-\hat{\eta}(t)\|\leq C\varepsilon,$$

for a constant $C>0$. In particular, for $\eta_1^m\equiv\eta_1$, system (8) is a global exponential observer for system (4)–(5).

Proofs of all previous theorems may be found in [6]. In the sequel, the system (4)–(5) will be often called as the master while (8) as the slave.

2.2. Parameter mismatch influence on the GLS synchronization

The following proposition analyzes the influence of mismatching the parameter τ in the master and slave when the master (4)–(5) with chaotic behavior is considered. Moreover, with a slight abuse of terminology, we assume here that "parameter" τ may be time dependent what will be used in the sequel when analyzing security of our encryption method.

Proposition 5. Consider system (8) with $\eta_1=\eta_1^m$, $\tau=\tau_{sl}(t)$ and system (4)–(5) with $\tau=\tau_{mast}(t)$, 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

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

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

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

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

Proof. Denoting $e=(e_1,e_2,e_3)^\top=\eta-\hat{\eta}$, one can easily obtain subtracting (8) with $\eta_1=\eta_1^m$, $\tau=\tau_{sl}(t)$ from (4–5) with $\tau=\tau_{mast}(t)$

$$\dot{e}=\begin{bmatrix} l_1 & 1 & 0 \\ l_2 & 0 & (\lambda_2-\lambda_1)\eta_1 \\ 0 & 0 & \lambda_3 \end{bmatrix}e+\begin{bmatrix} 0 \\ (-\Theta(t))\eta_1^3/2 \\ \frac{\lambda_3-2\lambda_1}{2(\lambda_1-\lambda_2)}\Theta(t)\eta_1^2 \end{bmatrix}, \tag{11}$$

so that the relation (9) follows immediately. To prove the remaining estimates, let us realize first that the matrix

$$\left[\begin{array}{cc} l_1 & 1 \\ l_2 & 0 \end{array}\right], \quad l_1 < 0,\ l_2 < 0,$$

is the Hurwitz one and therefore there exists a suitable (2×2) matrix S solving the following Lyapunov matrix equation

$$\left[\begin{array}{cc} l_1 & 1 \\ l_2 & 0 \end{array}\right]^{\top} S + S \left[\begin{array}{cc} l_1 & 1 \\ l_2 & 0 \end{array}\right] = -I_2,$$

I_2 being the (2×2) identity matrix. Now, consider the following Lyapunov function candidate

$$V(e) = [e_1, e_2] S \left[\begin{array}{c} e_1 \\ e_2 \end{array}\right] + \frac{1}{2} e_3^2,$$

then by straightforward computations

$$\frac{\mathrm{d}V}{\mathrm{d}t} = -e_1^2 - e_2^2 + \lambda_3 e_3^2 + e_3 \frac{\lambda_3 - 2\lambda_1}{2(\lambda_1 - \lambda_2)} \Theta(t) \eta_1^2 + 2[e_1, e_2] S \left[\begin{array}{c} 0 \\ e_3(\lambda_2 - \lambda_1)\eta_1 + \Theta(t)\eta_1^3/2 \end{array}\right].$$

Notice that by (9)

$$\frac{\mathrm{d}(e_3^2/2)}{\mathrm{d}t} = -\lambda_3 e_3^2 + e_3 \frac{\lambda_3 - 2\lambda_1}{2(\lambda_1 - \lambda_2)} \Theta(t) \eta_1^2$$

and therefore there exists $T > 0$, such that

$$|e_3| \leq \frac{\lambda_3 - 2\lambda_1}{2(\lambda_1 - \lambda_2)} \overline{\Theta} \eta_1^2 / \lambda_3 \leq \frac{\lambda_3 - 2\lambda_1}{2(\lambda_1 - \lambda_2)} \overline{\Theta} R^2 / \lambda_3, \quad \forall\, t \geq T.$$

Therefore, straightforward computations give $\forall\, t \geq T$ that

$$\left\| \frac{\mathrm{d}V}{\mathrm{d}t} \right\| \leq -e_1^2 - e_2^2 + \lambda_3 e_3^2 + \left(\frac{\lambda_3 - 2\lambda_1}{2(\lambda_1 - \lambda_2)} \right)^2 \overline{\Theta} R^4 / \lambda_3$$

$$+2(|s_{11}|e_1| + |s_{21}|e_2|) \left[\frac{(\lambda_2 - \lambda_1) \frac{\lambda_3 - 2\lambda_1}{2(\lambda_1 - \lambda_2)} \overline{\Theta} R^3}{\lambda_3} + \frac{\overline{\Theta} R^3}{2} \right]$$

$$:= -e_1^2 - e_2^2 + \lambda_3 e_3^2 + \alpha(\overline{\Theta})|e_1| + \beta(\overline{\Theta})|e_2| + \gamma(\overline{\Theta}), \quad \text{i. e.}$$

$$\left\| \frac{\mathrm{d}V}{\mathrm{d}t} \right\| \leq -(e_1 - \alpha/2)^2 - (e_2 - \beta/2)^2 + \lambda_3 e_3^2 + \gamma + \frac{\alpha^2 + \beta^2}{4}.$$

The last inequality means that the Lyapunov-like function $V(e)$ strictly decreases along any trajectory $e(t)$ until this trajectory enters ellipsoid $\mathcal{E}$ given by (recall that by (2) $\lambda_3 < 0$)

$$(e_1 - \alpha/2)^2 + (e_2 - \beta/2)^2 - \lambda_3 e_3^2 \leq \gamma + \frac{\alpha^2 + \beta^2}{4}.$$

As a consequence, any trajectory enters the set where

$$V(e) \leq \max_{e \in \mathcal{E}} V(e)$$

and stays within it forever. Now, the crucial observation is that for sufficiently small $\overline{\Theta}$ it holds

$$|\alpha(\overline{\Theta})| < \delta\overline{\Theta}, \quad |\beta(\overline{\Theta})| < \delta\overline{\Theta}, \quad |\gamma(\overline{\Theta})| < \delta\overline{\Theta},$$

where $\delta > 0$ is a suitable fixed real number. Therefore, the above ellipsoid $\mathcal{E}$ is fully located inside the ball of radius $\tilde{C}\overline{\Theta}$, where $\tilde{C} > 0$ is a real constant. In other words, $e(t)$ should ultimately stay within the set where $V(e) \leq \max_{\|e\| \leq \tilde{C}\overline{\Theta}} V(e)$ which ensures the existence of constant $C > 0$ required by the formulation of Proposition 5. The proof is complete. □

Remark 6. Using the technique of the above proof, one can obtain more specific estimate for the constant C given in the formulation of Proposition 5. This constant would be bigger if the mentioned bound R on the first component of the chaotic master system is bigger[1] and smaller, when observer gains $l_{1,2}$ and eigenvalue λ_3 have bigger absolute values. Important security feature of GLS is that λ_3 can not be affected, so that parameter mismatch would always have certain minimal influence despite choosing high gains l_1, l_2 in the observer (8). Moreover, equality (9) shows that for mismatched constant parameters τ_{mast}, τ_{sl} the absolute value of the third error component $e_3(t)$, even with $e_3(0) = 0$, becomes quickly strictly positive, with rate of increase being proportional to constant parameter mismatch $\overline{\Theta}$. As a matter of fact, (9) is the simple one dimensional asymptotically stable linear system forced by sign-preserving signal of magnitude proportional to constant parameter mismatch $\overline{\Theta}$. This feature is also crucial for our ACSK method presented later on since it provides the mentioned anti-synchronization effect. Proposition 5, as well as this remark, are supported and illustrated by numerous simulations experiments later on.

The following proposition will provide the estimate of the anti-synchronization effect mentioned at the end of the previous remark.

Proposition 7. Consider system (8), with $\eta_1 = \eta_1^m$, $\tau = \tau_{sl}$ and system (4)–(5) with $\tau = \tau_{mast}$, where τ_{sl}, τ_m are constants and some gains $l_1 \leq -1, l_2 \leq -1$ are fixed. Further, let it holds for some state trajectory $\eta(t) = [\eta_1(t), \eta_2(t), \eta_3(t)]^\top$ of (4)–(5)

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

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

$$|\eta_1(t) - \hat{\eta_1}(t)| \geq \frac{E^3}{12}\Theta t^2, \quad |\eta_2(t) - \hat{\eta_2}(t)| \geq \frac{E^3}{6}\Theta t,$$

[1] Actually, one can see that there is even dependence on R^3, so that the influence of the attractor size is crucial.

where

$$\Theta := |\tau_{mast} - \tau_{sl}|$$

and $\hat{\eta}(t)$ is any trajectory of (8) with $\hat{\eta}(0) = \eta(0)$.

P r o o f. Obviously, the error dynamics (11) holds again with $\Theta(t) :\equiv \overline{\Theta} = \tau_{mast} - \tau_{sl}$, namely

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

where $e(t) :\equiv \hat{\eta}(t) - \eta(t)$. Denote

$$\widetilde{A} = \begin{bmatrix} l_1 & 1 \\ l_2 & 0 \end{bmatrix} \tag{12}$$

and recall that by the assumption of the proposition being proved it holds $e(0) = \hat{\eta}(0) - \eta(0) = 0$. Then

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

$$\begin{bmatrix} e_1(t) \\ e_2(t) \end{bmatrix} = \int_0^t \exp(\widetilde{A}(t-s)) \begin{bmatrix} 0 \\ (\lambda_2 - \lambda_1)\eta_1(s)e_3(s) - \Theta\eta_1^3(s)/2 \end{bmatrix} \mathrm{d}s.$$

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

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

as a consequence

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

Further,

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

$$|\alpha(s)| = \left|(\lambda_2 - \lambda_1)e_3(s) - \Theta\eta_1^2(s)/2\right||\eta_1(s)| \ge \left|\Theta\eta_1^2(s)/2 - (\lambda_1 - \lambda_2)|e_3(s)|\right||\eta_1(s)|$$

$$\ge \left|E^2/2 - R^2(2\lambda_1 - \lambda_3)s\right|E\Theta/2, \quad \forall\, s \in [0, T^*].$$

Actually, one can easily check that $\forall\, s \in [0, T^*]$ it holds

$$E^2/2 - R^2(2\lambda_1 - \lambda_3)s \ge 0$$

i. e. one can use

$$|A+B| \geq ||A|-|B|| \geq |C-D|$$

for all real numbers A, B, C, D, such that $|A| \geq C, |B| \leq D, C \geq D$. Further, the straightforward computations show that for all $s \in [0, T^*]$

$$|\alpha(s)| \geq \Big|1-(R/E)^2(2\lambda_1-\lambda_3)s\Big|\Theta E^3/2 \geq |E^3/2-E^3/6|\Theta = \Theta E^3/3, \quad \text{i. e.}$$

$$|\alpha(s)| \geq \Theta E^3/3, \quad \forall\, s \in [0, T^*]. \tag{13}$$

Summarizing, to obtain the desired lower estimate for $e_1(t)$ and $e_2(t)$ one can use

$$\begin{bmatrix} e_1(t) \\ e_2(t) \end{bmatrix} = \int_0^t \exp(\widetilde{A}(t-s)) \begin{bmatrix} 0 \\ \alpha(s) \end{bmatrix} \mathrm{d}s = \int_0^t \exp(\widetilde{A}(s)) \begin{bmatrix} 0 \\ \alpha(t-s) \end{bmatrix} \mathrm{d}s, \tag{14}$$

$\forall\, t \in [0, T^*]$, where $\widetilde{A}$ is given by (12), while $\alpha(t)$ by (13). This implies easily

$$e_1(t) = \int_0^t \alpha(t-s)\big[s + l_1 s^2/2 + (l_1^2+l_2)s^3/6 + \cdots\big]\mathrm{d}s,$$

$$e_2(t) = \int_0^t \alpha(t-s)\big[1 + l_2 s^2/2 + (l_1 l_2)s^3/6 + \cdots\big]\mathrm{d}s,$$

$$|e_1(t)| = (1/3)\Theta E^3\big[t^2/2 + l_1 t^3/6 + (l_1^2+l_2)t^4/24 + \cdots\big]\mathrm{d}s$$

$$\geq (1/6)\Theta E^3 t^2\big[1 + l_1 t/3 + (l_1^2+l_2)t^2/12 + \cdots\big] \geq (1/12)\Theta E^3 t^2,$$

$$|e_2(t)| = (1/3)\Theta E^3\big[t + l_2 t^3/6 + (l_1 l_2)t^4/24 + \cdots\big]\mathrm{d}s$$

$$\geq (1/3)\Theta E^3 t\big[1 + l_2 t^2/6 + (l_1 l_2)t^3/24 + \cdots\big] \geq (1/6)\Theta E^3 t^2,$$

so that the claim to be proved follows. □

Remark 8. The essence of the anti-synchronization method to be described later on is to detect the anti-synchronization as soon as possible. Therefore, one can actually limit the previously proved proposition to a very small time interval. It is also intuitively clear, as well as rigorously shown during the above proof by the exact arguments, that smaller time interval, the faster anti-synchronization effect. Actually, following the above proof, infinitesimally for $t \to 0$, the above estimates provided by Proposition 7 may be replaced by the following ones:

$$|\eta_1(t) - \hat{\eta_1}(t)| \geq \frac{E^3}{4}\Theta t^2 + o(t^3), \quad |\eta_2(t) - \hat{\eta_2}(t)| \geq \frac{E^3}{2}\Theta t + o(t^3).$$

Moreover, the estimates of time T^* for the any reasonable system parameters and gains are much bigger that actually used in our algorithm later on. These time estimates were chosen to facilitate the proposition formulation. Notice also, that on a very short time interval the values E and R are close each to other (recall, that E is the minimal while R is the maximal absolute value of η_1 on some time

interval). The important quantity is E, see Table later on where distribution of E is studied. Actually, the speed of anti-synchronization depends on E^3! It also depends, though linearly only on parameter τ mismatch Θ. Finally, the most important observation here is that anti-synchronization is much better visible on e_2, rather than on e_1. Our algorithm later on will therefore use numerical derivation of e_1 combined with equation (11) to achieve e_2 (recall, that only η_1 is transmitted through the communication channel).

3. ANTI-SYNCHRONIZATION CHAOS SHIFT KEYING SCHEME

3.1. CSK and ACSK secure encryption schemes

As already mentioned, the anti-synchronization detection analyzed in the previous section will be used to design the realistic encryption and decryption algorithms. Namely, the well known CSK scheme will be modified. The classical CSK was first proposed by [14, 22] and its basic idea is to encode digital symbols with chaotic basis signals. Therefore, switching of chaotic modes provides quite simple configuration of the transmitter/receiver. However, as noted already in [14], synchronization is lost and recovered every time the transmitted symbol is changed. In the other words, the classical CSK receiver method needs during switching quite a time for an establishment of synchronization between the transmitter and the receiver, therefore speed of data transmission is rather poor while amount of data to encrypt a single bit quite huge. On the contrary, our novel approach that sharply improves these vital characteristics consists in using anti-synchronization rather than synchronization and will be further referred as the anti-synchronization CSK (ACSK) scheme. Its chart is shown in Figure 1 where public channel is used to send encrypted messages while secure channel a secret key.

On the transmitter side, there is the signal generator being the GLS (4)–(5) depending on crucial bifurcation parameter τ [5, 10, 24]. 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 suitable selected GLS bifurcation parameters from its known chaotic range, cf. [5, 6, 10, 24]. Then, only the first component of a chaotic signal $\eta_1 = x_1 = z_1 - z_2$ is being transmitted through the communication channel.

On the receiver side, signal $\eta_1 = x_1 = z_1 - z_2$ is feeded 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 *anti-synchronization* 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[2] 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 comparing 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 receiving the next piece of cipher text (i. e., the synchronizing signal $\eta_1(t)$)

[2]MATLAB–SIMULINK ode4 Runge–Kutta procedure with the fixed step size equal to 0.001 is being used throughout the paper.

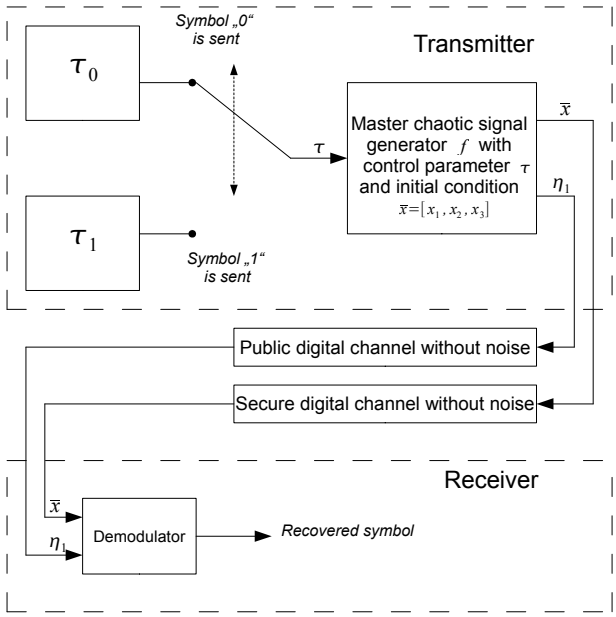

Fig. 1. ACSK digital communication system with anti-synchronization-error-based demodulator.

both slaves are again synchronized to the same best possible level of the "numerical zero" 10^{-4}.

As a matter of fact, as shown by Propositions 5, 7, for the fixed parameter mismatch $\Theta = |\tau_{mast} - \tau_{sl}|$ the anti-synchronization 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 anti-synchronization is to be detected. This crucial value has been experimentally thoroughly analyzed and their percent summary is given in Table.

Table.

E	$P(E)$	E	$P(E)$	E	$P(E)$
4.0	19.5	0.8	71.45	0.33	86.12
3.0	28.14	0.6	78.32	0.3	87.44
2.0	38.18	0.5	81.25	0.2	88.87
1	64.76	0.4	84.44	0.1	95.07

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

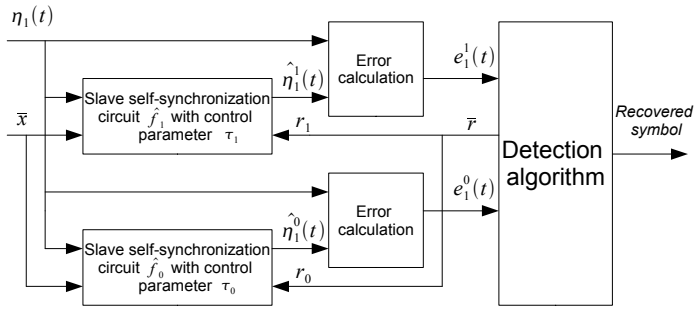

Fig. 2. Anti-synchronization-error-based ACSK demodulator.

3.2. Methods of the detection of the binary symbols in the receiver of the ACSK scheme

The receiver or demodulator structure of the ACSK scheme is shown in Figure 2 in a more detail. It detects the correct bit via identifying the correct synchronization signal and then rewrites its value into both self-synchronization circuits (see the back arrows r_0, r_1 in Figure 2). Such a detection in the receiver is based on the effect of the anti-synchronization, namely, two methods of the detection of the binary symbols are possible.

The first method that was proposed and studied in [7, 8] is based on the comparison of the absolute value of the first component of the synchronizing error e_1 in the receiver and the threshold value of the error. The threshold value is well-known and depends on the control parameters τ_1 and τ_0, gains, step size and solver. Depending on the $|\tau_1 - \tau_0|$ and the absolute value of the synchronizing signal η_1 various numbers of the iterations are needed to detect the binary symbol exactly. Sections with higher absolute value of the synchronizing signal η_1 is more convenient. The higher absolute value of η_1, the fewer iterations for the anti-synchronization effect are needed, and vice versa. It was shown in [8] that for quite close each to other chaotic generators with difference in τ_0 and τ_1 equal to 0.01 13 iterations were needed to distinguish the right slave subsystem from the wrong one. Nevertheless, those 13 iterations were needed for the detection of the single bit only when $|\eta_1(t)| \geq 4$. Otherwise, the correct detection requires even more iterations. The section of $\eta_1(t)$ signal where one can effectively decode the information using 13 iterations only equals to 19.5 percent of the total length of the ciphertext (see Table). Data rate of this method is therefore 15 bits/1000 iterations only, provided only section with $|\eta_1(t)| \geq 4$ is being used. Such a drawback suggests the necessity to look for a more precise analysis of the synchronization error, thereby further minimizing the iteration number needed for 1 bit encryption/decryption.

The second method of the detection of the binary symbols in the receiver is based on the comparison of the value of the second component of the error e_2 and was first briefly introduced in [9]. Now, this method is justified by the theoretical analysis presented in the previous section. Actually, Proposition 7 shows that, while the first component of the synchronization error peak triggered by the parameter mismatch is of order $O(t^2)$, the peak of its second component is of the order $O(t)$. For very small t (note, that one iteration is typically per time equal to 0.001) this is a really significant difference. As all data are transferred precisely in the digital form, they don't contain any noise and we can use simple derivative observer to predict the second component of the error. In such a way, the parameter mismatch can be detected almost immediately, looking on a single subsequent iteration only (for $|\eta_1(t)| \geq 4$). As a consequence, this second method can decrypt/encrypt efficiently 195 bits/1000 iterations. Let us note here, that in [9] it was reported that for the correct detection of the wrong slave synchronization circuit in the receiver only one iteration is needed for $|\eta_1(t)| \geq 2$. Nevertheless, a recent and more careful experimental analysis shows that the threshold of the safe detection should be increased to $|\eta_1(t)| \geq 4$. The reason is that the number of the iterations needed for the correct bit identification depends on the speed of the change of the synchronization signal $\eta_1(t)$, too. When the synchronization signal is increasing/decreasing very fast, one iteration for the correct detection is insufficient. Nevertheless, bit rate can be yet further improved as other signal $\eta_1(t)$ sections can be used subsequently with $2, 3$ and 4 iterations (the last one even for $|\eta_1(t)| \approx 0.1$!), thereby using up to 95% of this signal, cf. Table.

3.3. Comparison of detection methods

Both methods may be illustrated and compared using Figure 3 where the second graph from top shows evolution of the synchronization error component e_1 while the third from the top graph shows the evolution of the synchronization error component e_2. Notice that the values of peaks of e_1 can not be safely distinguished numerically as correct and non-correct values differ by a negligible small margin, namely level of e_1 for the correct first bit is about 1.52×10^{-4} while for the non-correct first bit only 1.525×10^{-4}. Nevertheless, one can trace from the picture sudden change of the derivative of e_1 which indicates the non-correct bit. As a matter of fact, the reconstructed second component e_2 is mainly driven by the time derivative e_1. Therefore, for the correct bit e_2 it is approximately 2×10^{-3} while for non-correct bit it is approximately 10^{-2} which is easily distinguishable. Such a difference is produced even during a single iteration what makes the second detection method much more efficient than the first one as already noted at the end of the previous subsection where estimates of the corresponding bit rates are discussed.

4. NUMERICAL EXPERIMENTS

Example of the application of the current ACSK method is shown in Figure 3. It shows an example of a transmitted baseband signal for the message "0110110010" encoded by means of two different, but close each to other chaotic GLS generators with different parameters $\tau_0 = 0.1$ and $\tau_1 = 0.2$. Only ciphertext is available to

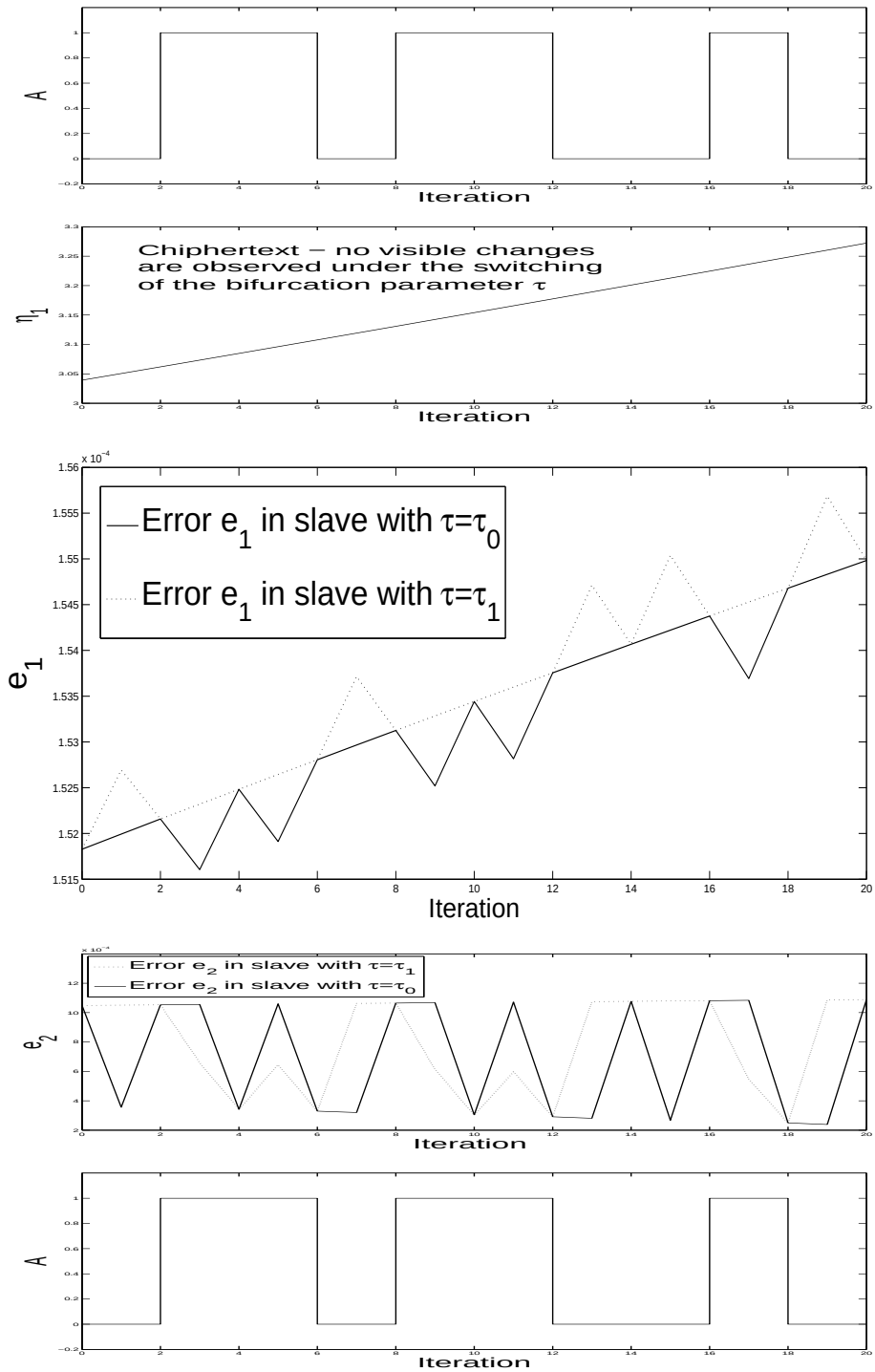

Fig. 3. Time histories related with the encryption and decryption of the plaintext "0110110010" using the ACSK method. From up to down: plaintext time signal; ciphertext $\eta_1(t)$; $e_1(t)$; $e_2(t)$ and the reconstructed plaintext.

potential intruder with no clue of encrypted signal. This ciphertext is the synchronizing signal $\eta_1(t)$ sent by GLS either with $\tau_0 = 0.1$ or $\tau_1 = 0.2$, depending on an encrypted value of the current bit. For the easy mutual comparison of all scopes in Figure 3, their time axes are identical and indicate number of iterations[3], not a real time. It can be seen that the error immediately (during one iteration only) rises in one of the slaves, while in the other one it remains within declared "numerical zero" $\sim 10^{-4}$. Though each symbol in Figure 3 requires two iterations, the method works perfectly even with a single iteration only (the second iteration is needed just to reset the initial conditions in "the wrong" slave to the initial conditions in "the true" slave.). The ciphertext obviously does not indicate change of bits in any way. There are two reasons: first, the parametrization with respect to τ makes it possible to have signals of both chaotic systems close to each other. Secondly and most importantly, as we use 1–2 bits only, it is impossible to estimate any statistical or other tendency to decrypt the information. The decryption is possible only by feeding the ciphertext into slave systems producing peaking error picture shown in Figure 3, which clearly decrypts the corresponding digital information.

Notice that the previously presented Chaos Shift Keying method, [14, 22], typically needs up to one 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 ACSK, 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.

5. SECURITY ANALYSIS OF ACSK METHOD

The above described decryption scheme in the ACSK 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 in the sense that two initial conditions closer 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 $\eta_2(t)$ easily obtained by 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 5 implies that at least 10 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 plain text and the corresponding cipher text, but

[3]Recall, that the "iteration" is one step of the Runge–Kutta 4th order scheme with the fixed step 10^{-3}

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^{10000} 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 can not see any clue of changing parameter when analyzing signal η_1. Nevertheless, the difference $|\tau_0 - \tau_1|$ can not be arbitrarily small, as the anti-synchronization effect depends on this difference as well, see Propositions 5, 7. 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 [4]. Finally, notice that secret key based on parameter τ is equally resistant even in 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 one. 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 second equation in (11). Indeed, τ mismatch level Θ and initial error $e_3(0)$ influence are mixed on the right hand side there, and nonzero value of any of them spoils a possible detection.

More rigorous security analysis is matter of ongoing investigation, but the above draft analysis indicates promising potential of the ACSK method.

6. CONCLUSIONS AND OUTLOOKS

The anti-synchronization properties of the generalized Lorenz system family has been analyzed and used for the anti-synchronization detection in ACSK scheme. It was shown that the resulting ACSK digital communication method has potential of introducing a high degree of security at a low receiver complexity. At the same time, it requires reasonable amount of data to encrypt a single bit, thereby making revolutionary possibility of practical and realistic use of continuous time chaotic

system for digital data encryption. Further research will be devoted to making the message expansion even smaller.

ACKNOWLEDGEMENT

This work was supported by the Czech Science Foundation through the research grant no. 102/08/0186.

(Received April 4, 2009)

REFERENCES

[1] J. Alvarez, H. Puebla, and I. Cervantes: Stability of observer-based chaotic communication for a class of Lur'e systems. Internat. J. Bifurcation Chaos *7* (2002), 1605–1618.

[2] G. Alvarez and S. Li: Cryptographic requirements for chaotic secure communications. arXiv: nlin. CD/0311039, 2003.

[3] T. L. Carroll and L. M. Pecora: Cascading synchronized chaotic systems. Physica D *67* (1993), 126–140.

[4] S. Čelikovský: Observer form of the hyperbolic-type generalized Lorenz system and its use for chaos synchronization. Kybernetika *40* (2004), 6, 649–664.

[5] S. Čelikovský and G. Chen: On a generalized Lorenz canonical form of chaotic systems. Internat. J. Bifurcation Chaos *12* (2002), 1789–1812.

[6] S. Čelikovský and G. Chen: Secure synchronization of chaotic systems from a nonlinear observer approach. IEEE Trans. Automat. Control *50* (2005), 76–82.

[7] S. Čelikovský, V. Lynnyk, and M. Šebek: Anti-synchronization chaos shift keying method based on generalized Lorenz system. In: Proc. The 1st IFAC Conference on Analysis and Control of Chaotic Systems. CHAOS'06, 2006, pp. 333–338.

[8] S. Čelikovský, V. Lynnyk, and M. Šebek: Observer-based chaos sychronization in the generalized chaotic Lorenz systems and its application to secure encryption. In: Proc. The 45th IEEE Conference on Decision and Control, 2006, pp. 3783–3788.

[9] S. Čelikovský and V. Lynnyk: Anti-synchronization chaos shift keying method: Error derivative detection improvement. In: Proc. The 2st IFAC Conference on Analysis and Control of Chaotic Systems. CHAOS '09, pp. 1-6.

[10] S. Čelikovský and A. Vaněček: Bilinear systems and chaos. Kybernetika *30* (1994), 403–424.

[11] K. M. Cuomo and A. V. Oppenheim: Circuit implementation of synchronized chaos with application to communications. Physical Rev. Lett. *71* (1993),1, 65–68.

[12] K. Cuomo, A. Oppenheim, and S. Strogatz: Synchronization of Lorenz-based chaotic circuits with applications to communications. IEEE Trans. Circuits and Systems II *40* (1993), 626–633.

[13] F. Dachselt and W. Schwartz: Chaos and cryptography. IEEE Trans. Circuits and Systems I *48* (2001), 1498–1509.

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

[15] L. Gamez-Guzman, R. M. Cruz-Hernandez, Lopez-Gutierrez, and E. E. Garcia-Guerrero: Synchronization of Chua's circuits with multi-scroll attractors: Application to communication. Communications in Nonlinear Science and Numerical Simulation *14* (2009), 6, 2765–2775.

[16] J. M. V. Grzybowski, M. Rafikov, and J. M. Balthazar: Synchronization of the unified chaotic system and application in secure communication. Communications in Nonlinear Science and Numerical Simulation *14* (2009), 6, 2793–2806.

[17] L. Kocarev and U. Parlitz: General approach for chaotic synchronization with applications to communications. Phys. Rev. Lett. *74* (1995), 25, 5028–5031.

[18] L. Kocarev: Chaos-based cryptography: a brief overview. Circuits Systems Magazine *1* (2001), 6–21.

[19] A. A. Koronovskii, O. I. Moskalenko, P. V. Popov, and A. E. Hramov: Method for secure data transmission based on generalized synchronization. BRAS: Physics. *72* (2008), 1, 131–135.

[20] K. Lian and P. Liu: Synchronization with message embedded for generalized Lorenz chaotic circuits and its error analysis. IEEE Trans. Circuits Systems I *47* (2000), 1418–1424.

[21] U. Parlitz, L. Kocarev, T. Stojanovski, and H. Preckel: Encoding messages using chaotic synchronization. Phys. Rev. E. *53* (1996), 4351–4361.

[22] U. Parlitz, L. O. Chua, L. Kocarev, K. S. Halle, and A. Shang: Transmission of digital signals by chaotic synchronization. Internat. J. Bifur. Chaos *2* (1992), 973–977.

[23] R. Schmitz: Use of chaotic dynamical systems in cryptography. J. Franklin Inst. *338* (2001), 4, 429–441.

[24] A. Vaněček and S. Čelikovský: Control Systems: From Linear Analysis to Synthesis of Chaos. Prentice-Hall, London 1996.

[25] A. R. Volkovskii and N. Rulkov: Synchronouns chaotic response of a nonlinear oscillating system as a principle for the detection of the information component of chaos. Tech. Phys. Lett. *19* (1993), 97–99.

Volodymyr Lynnyk, Department of Control Engineering, Faculty of Electrical Engineering, Czech Technical University in Prague, Technická 2, 166 36 Praha 6 and Institute of Information Theory and Automation, Academy of Sciences of the Czech Republic, Pod Vodárenskou věží 4, 182 08 Praha 8. Czech Republic.

e-mail: voldemar@utia.cas.cz

Sergej Čelikovský, Institute of Information Theory and Automation, Academy of Sciences of the Czech Republic, Pod Vodárenskou věží 4, 182 08 Praha 8 and Department of Control Engineering, Faculty of Electrical Engineering, Czech Technical University in Prague, Technická 2, 166 36 Praha 6. Czech Republic.

e-mail: celikovs@utia.cas.cz