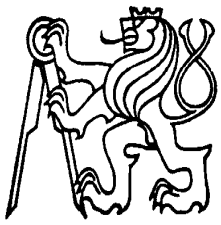
ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ
Fakulta elektrotechnická



CZECH TECHNICAL UNIVERSITY
Faculty of Electrical Engineering

RNDr. Sergej Čelikovský, CSc.

Synchronizace chaotických oscilatorů pomocí nelineární rekonstrukce a její využití k bezpečnému šifrování

Chaos synchronization via nonlinear observers with application to secure encryption

Summary

During previous decades, chaotic systems has been subjected to intensive research, in particular, using the methods of the automatic control theory. One of the prominent problems here is the so-called synchronization of two or more chaotic systems. Even in case, when having two identical copies of the same chaotic system with practically the same initial conditions, thanks to strong dependence on initial data, after some time their behavior may be very different. In such a way, chaotic oscillations tends to be de-synchronized, unless some synchronizing influence is being imposed. Synchronization is usually achieved by transferring certain synchronizing signal from one chaotic system into the other one. This signal should have the least possible dimension, preferable it should be a scalar time function. As a suitable theoretical framework for synchronization appears to be the notion of the observer introduced by automatic control theory. Synchronized chaotic systems may be used for various secure encryption schemes. For such a purpose, one of those synchronized chaotic systems is used on the transmitter side to encrypt the sensitive information while the other one is used on the receiver side to decrypt it. In this case, the notion of the so-called secure synchronization is important. The secure synchronization is the one which can be achieved only when knowing some crucial system parameter information. Such an information may later serve as a secure password. This lecture will give brief overview of possible secure encryption/decryption methods based on synchronized chaotic systems. Furthermore, it will define the above indicated secure synchronization and it will introduce the special class of chaotic systems, together with its efficient parametrization enabling even the global exponential synchronization. Such a synchronization is based on nonlinear transformations and subsequent observer design having favorable error dynamics. Moreover, its security may be investigated thanks to the mentioned parametrization as well.

Souhrn

Chaotické systémy jsou v posledních desetiletích intenzivně zkoumány i metodami teorie automatického řízení. Jedním z důležitých problémů je zde synchronizace dvou, či více chaotických systémů. Dokonce i tehdy, když se bude jednat o dvě kopie téhož dynamického systému, které budou inicializovány ve stejný okamžik z prakticky stejných počátečních podmínek, budou se příslušné oscilace po určité době rozcházet v důsledku známého efektu citlivé závislosti chaotických oscilací na počátečních podmínkách. Synchronizace je proto možné dosáhnout jedině působením synchronizujícího signálu předávaného z jednoho systému do druhého. Vhodným teoretickým rámcem z oboru teorie řízení se proto jeví pojem pozorovatele, kdy synchronizující signál budeme považovat za měřený výstup prvního systému a druhý systém bude asymptotickým pozorovatelem prvního systému na základě zmíněného měřeného výstupu. Důležitým aspektem pro praktické využití je, aby výstup byl pokud možno co nejužší částí stavu, nejlépe jednorozměrným signálem. V tomto případě jsou pak synchronizované chaotické oscilátory využitelné celou řadou šifrovacích metod. Všechny tyto metody mají společné využití skrytých komponent stavu, které nejsou veřejně předávány, avšak mohou být na straně příjemce zrekonstruovány pomocí synchronizace. Je proto nasnadě, že při všech těchto postupech je důležitou vlastností tzv. bezpečnost synchronizace. Zjednodušeně řečeno, bezpečná synchronizace je taková synchronizace, která je možná jen při přesné znalosti některého klíčového parametru systému, který je pak vhodným kanditátem na generování hesel příslušné šifrovací metody. V této přednášce bude jednak podán stručný přehled možných šifrovacích metod založených na synchronizovaném chaosu, dále pak budou odvozeny některé konkrétní třídy systémů, které je možné bezpečně synchronizovat pomocí nelineární rekonstrukce, založené na metodě nelineárních transformací a následné přesné linearizaci chybové dynamiky.

Klíčová slova: Nelineární rekonstrukce, synchronizace chaosu, šifrování.

Keywords: Nonlinear observers, chaos synchronization, secure encryption.

Contents

1 Introduction

Beginning with [46], synchronization of chaotic systems has now become a popular research topic [1, 2, 8, 23, 27, 33, 47, 50, 51, 53], where, in particular, ideas from control theory find a natural practice. Along this line of research, it should be noted that an even broader problem of synchronization of nonlinear oscillations has already had a long history with a great variety of applications (see [6] for an informative survey).

The present lecture aims to discuss the full (or complete) synchronization problem, i.e., when all state trajectories of the synchronized systems mutually asymptotically converge as time goes to infinity. For partial synchronization, see [51, 47] and the references cited therein. The full synchronization problem is naturally close to the observer concept in control systems theory [42], and have found various applications including the secure communication problem to be further discussed later on.

To start, it is worth pointing out that one may view synchronization as a specified version of a general observer design problem, since the system output may be freely selected by the designer, which however should have the smallest possible dimension preferably using only one scalar signal.

An important aspect of synchronization is its security. Interest in synchronization has been boosted mainly by its possible use for chaos-based secure communication and encryption. The chaotic system used on the transmitter side is for encrypting the message, which is then transmitted through an open channel, and then another synchronized copy of the same chaotic system on the receiver side is used to decrypt it. Various encryption-decryption methods may be used (see, e.g., [17] for an overview). A crucial property of chaotic systems is their sensitive dependence on initial conditions, so that the asymptotic synchronization is inevitable for the scheme, which is supposed to prevent messages from being read during the transmission process by any intruder. Some initial values and/or parameters of the chaotic transmitter system are used as the "password" and it is believed that without their precise knowledge an intruder would not be easy or practically unable to read the hidden messages. Although this approach may not be the best possible in theory, it has many merits for practical applications where a trade-off between security and commercial requirements (e.g., cost and convenience of operations) is deemed necessary.

From the viewpoint of systems theory, it may seem obvious that many robust and adaptive control methods could be considered for possible attacks against secure communication and encryption schemes. Unfortunately, this problem was largely ignored when synchronization-based communication schemes were suggested in the past. In particular, there is such a typical case of using a general Lur'e system to synchronize its identical copy (see, e.g., [2]), but as will be seen here there is a simple way to practically synchronize two representative Lur'e systems with different nonlinearities, which implies that the use of Lur'e chaotic systems for secure communication could be questionable.

In this lecture, the secure synchronization will be introduced and its relation to all known secure encryption chaos based techniques will be discussed. To do so, description of these techniques will be given as well. Further, a class of chaotic systems will be suggested to overcome the aforementioned drawbacks. More precisely, it will be shown that for a large class of chaotic systems the error in the knowledge of system parameters implies an unremovable synchronization error of the same magnitude; this implies that a small enough non-matching parameters error will *never* spoil the synchronization (i.e., the robustness in the usual sense) while a big enough error will *always* spoil it (i.e., the so-called anti-robustness to be defined below).

This class of systems is the so-called *generalized Lorenz system*, introduced in [10, 55] and then extended and further studied in detail in [11]. The generalized Lorenz system is a signifi-

cant generalization of the well-known classical Lorenz system, leading to a natural unification with the Chen system [9], which is a dual system of the Lorenz system [54, 1, 56, 36]. In [11], the canonical form of the generalized Lorenz system was developed to enable efficient generation of a variety of chaotic oscillations. Based on a special nonlinear transformation, the present lecture will further develop the global exponential synchronization scheme and then it will discus its security against various known attacks that use adaptive and robust control techniques. In such a way, a promising methodology for the chaos-synchronization-based secure communication, significantly improving most, if not all, existing schemes of this kind, is provided.

2 Secure encryption schemes based on chaotic systems

To motivate the mentioned problem of the secure synchronization of chaotic systems, let us first describe its most promising application. This application is the secure encryption of sensitive information. Despite variety of possible schemes there is common feature which is the involvement of two copies of the same chaotic systems that are mutually synchronized. The necessity of the synchronization follows from the well known property of chaotic system being strongly dependent of the choice of initial conditions (the famous "butterfly wing effect"). Thanks to it, two independent copies of the same chaotic system with almost same initial condition would present very different behavior after sufficiently long period of time. Therefore, a synchronizing connection is needed between those two identical chaotic systems to keep their synchronization.

All secure encryption schemes are based on the property that there is one of those synchronized chaotic systems on the transmitter side and the other one on the receiver side. First of them is used to encrypt while the other one to decrypt the sensitive information. As a secure password, the value of some vital parameter precisely defining the particular chaotic system is used. In other words, both the person sending the encrypted message and the person receiving it have at their disposal whole rich family of chaotic systems and the knowledge of a secure password enables them to choose precisely one of them.

Once having such a chaotic system, various scheme are possible. Despite the strong relevance of the discrete-value systems, there have been attempts to apply cryptographical methods to continuous-value information. Early investigations, that were mainly inspired by the increasing research on chaotic systems can be found in [57, 5, 38, 40, 25, 7, 4]. In these applications, autonomous chaotic systems were used as pseudo-random number generators in discrete-value implementations. Thereafter, the pioneering works on chaos synchronization, [52, 53, 56, 47, 50, 51, 55, 54, 46, 19], led to a new branch of applications. Now, nonautonomous chaotic systems with continuous-value signals were used to transmit information. Several schemes have been developed which allow to transform the information signal into a chaotic waveform on the encoder side and to extract the information signal from the transmitted waveform on the decoder side. The most important among them are:

- **Chaotic Masking:** The encoder consists of an autonomous chaotic system whose output signal is added to the information signal. This sum is transmitted over the channel. The decoder uses the transmission signal to synchronize an equivalent chaotic system with the encoder system. The reconstructed chaotic signal is then subtracted from the transmission signal which finally reconstructs the information signal. In order to guarantee synchronization on the receiver side the information signal has to be sufficiently small with respect to the chaotic signal.

- **Chaos Shift Keying (CSK):** The encoder consists of two or more autonomous chaotic

systems with different parameters. According to the discrete information signal one of them is selected whose output signal is transmitted over the cannel. In the decoder the same number of chaotic systems tries to synchronize with their encoder counterparts. The parameters are adjusted in such a way that only one pair can synchronize at a time. Detecting this synchronization decodes the discrete information.

- **Chaotic Modulation or Inverse System:** The encoder is a nonautonomous chaotic system whose state is influenced by the information signal. The decoder synchronizes with the encoder via reconstruction of its state using the transmission signal. The information signal is recovered by applying the inverse encoder operation to the reconstructed state and the transmission signal.

- **Anti-synchronization Chaos Shift Keying (ACSK):** As already mentioned, the classical CSK was first proposed by [43, 18] and its basic idea is to encode digital symbols with chaotic basis signals. Therefore, switching of chaotic modes provides quite simple configuration of the receiver. However, as noted already in [24], the classical CSK method needs during switching quite a long 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 is really huge. As an alternative, ACSK is proposed in [14, 16, 15]. Its chart is shown on Fig. 1, where public channel is used to send encrypted messages while secure channel a secret key. Secret key will consist of information[1] enabling to have full synchronization of transmitter and both receivers to

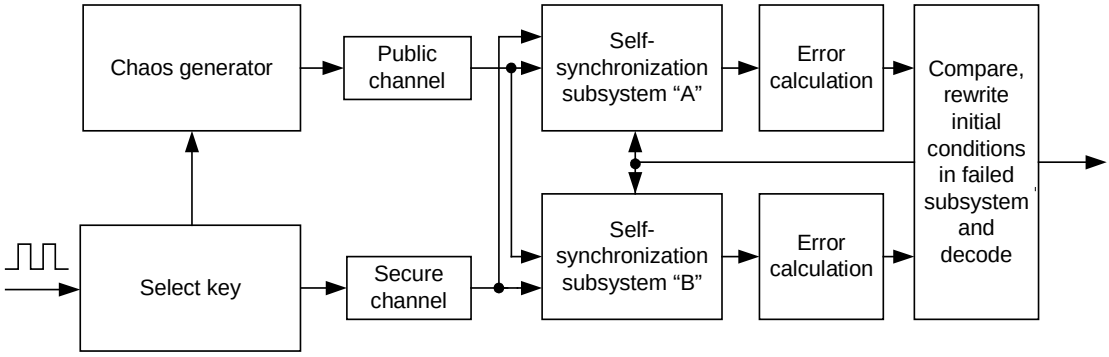


Figure 1: ACSK digital communications system with anti-synchronization-error-based demodulator. Public channel is used to send encrypted messages while secure channel a secret key.

reasonable extent. The synchronizing signal is feeded into both of them. After certain time, one of them, say “B”, produces significantly bigger error, what determines correct binary value as 0. At the end of the step, the state of oscillator ”“B” is reset to that of “A”, thereby maintaining all the time synchronization up to a required level. Then, next bit may be handled in the same way.

All of these schemes have been investigated analytically and experimentally in continuous-time as well as in discrete-time applications [59, 21, 44, 28, 34, 45, 61, 35, 26].

[1]This may be initial condition, or random length of time period during which we transmit synchronizing signal from **publicly known** constant zero information signal.

According to [17], the inverse-system approach [19] seems to be the most suitable scheme for continuous-value encryption because of its unrestricted signal structure. Furthermore, its structure corresponds to conventional self-synchronizing stream ciphers [39, 49]. Nevertheless, recent results on ACSK, [15, 16, 14], are promissing as well.

What qualifies chaos for encryption purposes? The interest in this application field is mainly triggered by the obvious geometrical signal complexity and the statistical signal properties which can be observed in nonlinear dynamical systems [30, 47, 60]. In this way, chaotic signals can be thought of as the continuous-value equivalent of discrete-value pseudo-random sequences which are discussed in conventional cryptography.

3 Synchronization as an observer design problem

As already noted, all mentioned encryption and decryption schemes are heavily dependent on the possibility of secure synchronization.

The main purpose of this part is to introduce the security of synchronization with respect to adaptive and robust control schemes; therefore, for brevity the discussion is limited to the static case and the simplest version of the adaptive observer.

Consider the following nonlinear system with a (possibly unknown) parameter vector μ ("password" candidate):

$$\dot{x} = f(x, t, \mu), \;\; x \in \mathbb{R}^n, \mu \in \mathbb{R}^m. \tag{1}$$

Definition 1 *System (1) is said to achieve a* static synchronization *of a solution $x(t)$, $t \geq t_0$, if there exists an auxiliary output, $y = h(x) \in \mathbb{R}^p$, $p < n$, such that with this output system (1) is the following smooth asymptotic observer for the solution $x(t)$, $t \geq t_0$:*

$$\dot{\widehat{x}} = f(\widehat{x}, t, \mu) + \varphi(h(x), h(\widehat{x}), \widehat{x}, \mu), \;\; x, \widehat{x} \in \mathbb{R}^n, \; \mu \in \mathbb{R}^m. \tag{2}$$

The synchronization is said to be anti-adaptive secure *with respect to parameter μ, if there does not exist any adaptive observer of the form (2) with $\mu = \widehat{\mu}$, where*

$$\dot{\widehat{\mu}} = \psi(\widehat{\mu}, h(x) - h(\widehat{x}), \widehat{x}, t), \;\; \widehat{\mu} \in \mathbb{R}^m.$$

Moreover, the synchronization is said to be anti-robust secure *with respect to parameter μ, if there exists a constant $K > 0$ such that for any $\overline{\mu}, \widetilde{\mu}$ from a given compact set and for any solution of (1) with $\mu = \overline{\mu}$ and (2) with $\mu = \widetilde{\mu}$, it holds that $\underline{\lim}_{t\to\infty} \|x(t) - \widetilde{x}(t)\|_{\mathbb{R}^n} \geq K(\overline{\mu} - \widetilde{\mu})$. The* secure synchronization *is defined to be one that is both anti-adaptive and anti-robust secure.*

Anti-robust security implies that big enough parameter mismatch should cause big enough synchronization error despite any observer used. To use synchronization for secure communication, both anti-robust and anti-adaptive security properties are crucial for resisting potential attacks. Obviously, they are very broadly defined here and therefore somewhat difficult to verify. As a matter of fact, it is believed that every practically implementable secure code is breakable, by an intruder having at his disposal sufficient amount of time and computing power [17]. Therefore, the security level is a matter of trade-off between the designers' costs and the customers' requirements. Nevertheless, security analysis is not the main concern of the present paper.

Some terminology has to be introduced first. *Scalar synchronization* is the one that uses a scalar auxiliary output for communication, *global synchronization* ensures the global convergence of any observed trajectory with any initial observation error, while *exponential synchronization* ensures exponential decay of synchronization errors.

Certainly, it is undesirable if a synchronization scheme is known to be vulnerable to simple attacks. Some cases, where the synchronization schemes are known to be insecure are listed and proved in [12]:

Proposition 1 *Suppose that system (1) and its synchronizing output $h(x)$ have the form*

$$\dot{x} = A(Cx,t)x + \varphi(Cx,t) + B\Phi(Cx,t)\left[\begin{array}{ccc} \alpha_1(\mu) & \cdots & \alpha_k(\mu) \end{array}\right]^\top, \qquad y = h(x) = Cx, \quad (3)$$

where $x \in \mathbb{R}^n$, $y \in \mathbb{R}^p$, $\mu \in \mathbb{R}^s$, $A(Cx,t)$ is an $(n \times n)$ matrix with uniformly Lipschitz entries, C is a $(p \times n)$ matrix, B is $(n \times k)$ matrix, and $\Phi(x)$ is a $(k \times k)$ symmetric matrix with uniformly Lipschitz entries. Assume that there exist positive definite and symmetric $(n \times n)$ matrix S, $(n \times p)$ matrix L, $(k \times p)$ matrix R, and a real number $T > 0$, such that for a given uniformly bounded solution $x(t)$, $t \geq t_0$, of (3),

$$S(A(Cx(t),t) + LC) + (A(Cx(t) + LC)^\top S < Q < 0, \ \ \forall t \geq T, \quad SB = C^\top R. \quad (4)$$

Then, the system allows synchronization of $x(t)$, $t \geq t_0$, which is not anti-adaptive secure; namely, it admits the following adaptive observer:

$$\begin{array}{rcl} \dot{\hat{x}} & = & A(Cx(t),t)\hat{x} + LC(\hat{x} - x) + \varphi(Cx,t) + B\Phi(Cx,t)\hat{p} \\ \dot{\hat{p}} & = & \Phi(Cx,t)RC(x - \hat{x}), \quad \hat{p} \in \mathbb{R}^k. \end{array}$$

The above proposition provides a multi-output generalization of the input-free version of Theorem 5.3.2 in [37], as the condition (4) follows from the well-known Kalman-Yacubovitch Lemma. Moreover, applying the persistency of excitation property (Lemma B.2.3 of [37]), one easily has the following result.

Corollary 1 *Anti-secure synchronization with password decoding. Suppose, in addition to the conditions of Proposition 1, that there exist two positive real constants T, K, such that along the synchronized system trajectory $x(t)$ it holds for all $t \geq t_0$ that*

$$\int_t^{t+T} \Phi^\top(Cx(\tau),\tau)B^\top B\Phi(Cx(\tau),\tau) \geq KI_{k\times k} > 0.$$

Then, $\hat{p}(t) \to p := [\alpha_1(\mu), \ldots \alpha_k(\mu)]^\top$ as $t \to \infty$.

If some of the parameters $\mu \in \mathbb{R}^s$ are used as the password, Proposition 1 gives an even possibility to decoding it, which makes attack fairly easy. It is worth noting that the persistency of excitation property may actually hold, thanks to the well-known properties of the chaos such as its topological transitivity.

Proposition 2 *Suppose that system (1) and its synchronizing output $h(x)$ have the form*

$$\dot{x} = \left[\begin{array}{cccc} x_2 & \cdots & x_n & \phi(x,\mu) \end{array}\right]^\top, \qquad h(x) = x_1,$$

where $\phi(x,\mu)$ is Lipschitz, x is bounded, and μ stays within a compact set. Then, the above system allows synchronization that is not anti-robust secure. Namely, the system

$$\dot{\hat{x}} = \left[\begin{array}{cccc} \hat{x}_2 & \cdots & \hat{x}_n & \phi(\hat{x},\mu_0) \end{array}\right]^\top + \left[\begin{array}{cccc} \theta & \theta^2 & \cdots & \theta^n \end{array}\right]^\top (x_1 - \hat{x}_1),$$

where μ_0 is some nominal value of the unknown parameter μ, has the property that for any $\varepsilon > 0$, there exists a $\theta(\varepsilon) > 0$, such that $\overline{\lim}_{t\to\infty}\|x(t) - \hat{x}(t)\| \leq \varepsilon$.

As a matter of fact, the above proposition shows that there exist systems, synchronizable using the robust observer technique up to any level despite the lack of knowledge of its parameters. Such a system is therefore synchronizable, but not securely and therefore it is not convenient for encryption purposes. This shows clearly that results of [2], suggesting certain secure encryption scheme, are rather controversial and superficial.

4 The generalized Lorenz system and its synchronization

Here, the specific class of chaotic systems will be introduced and studied to show that the above mentioned secure synchronization is achievable. This class of systems is the so-called generalized Lorenz system defined as follows.

Definition 2 *The following general nonlinear system of ordinary differential equations in $\mathbb{R}^3$ is called a generalized Lorenz system (GLS):*

$$\dot{x} = \begin{bmatrix} A & 0 \\ 0 & \lambda_3 \end{bmatrix} x + \begin{bmatrix} 0 \\ -x_1 x_3 \\ x_1 x_2 \end{bmatrix}, \quad A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}, \tag{5}$$

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

$$-\lambda_2 > \lambda_1 > -\lambda_3 > 0. \tag{6}$$

Moreover, the generalized Lorenz system 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.*

Motivation for studying this generalized Lorenz system has been thoroughly discussed in [55, 11]. In particular, the inequality condition (6) on the system eigenvalues is now well understood, in view of Shilnikov's criterion (see, e.g., Section 3.2 of [58]). Since the eigenvalues requirement (6) is the only one, the generalized Lorenz system represents a quite general class of autonomous systems in $\mathbb{R}^3$. The following result, enabling efficient synthesis of a rich variety of chaotic behaviors for GLS, has been obtained in [11]:

Theorem 1 *For the nontrivial generalized Lorenz system $(5) - (6)$, there exists a nonsingular linear change of coordinates, $z = Tx$, which takes (5) into the following generalized Lorenz canonical form:*

$$\dot{z} = \begin{bmatrix} \lambda_1 & 0 & 0 \\ 0 & \lambda_2 & 0 \\ 0 & 0 & \lambda_3 \end{bmatrix} z + cz \begin{bmatrix} 0 & 0 & -1 \\ 0 & 0 & -1 \\ 1 & \tau & 0 \end{bmatrix} z\,, \tag{7}$$

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

Synchronization of GLS is based on the following important result, which is a generalization of the result of [52], as the latter is applicable only to a very special form of matrix A.

Theorem 2 *Both nontrivial GLS (5) and its canonical form (7) are state equivalent to the following form:*

$$\frac{\mathrm{d}\eta}{\mathrm{d}t} = \begin{bmatrix} (\lambda_1 + \lambda_2)\eta_1 + \eta_2 \\ -\lambda_1\lambda_2\eta_1 - (\lambda_1 - \lambda_2)\eta_1\eta_3 - (1/2)(\tau+1)\eta_1^3 \\ \lambda_3\eta_3 + K_1(\tau)\eta_1^2 \end{bmatrix} \tag{8}$$

$$K_1(\tau) = \frac{\lambda_3(\tau+1) - 2\tau\lambda_1 - 2\lambda_2}{2(\lambda_1 - \lambda_2)}, \tag{9}$$

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*

$$\eta^\top = \left[z_1 - z_2, \;\; \lambda_1 z_2 - \lambda_2 z_1, \;\; z_3 - \frac{(\tau+1)(z_1 - z_2)^2}{2(\lambda_1 - \lambda_2)} \right] \tag{10}$$

$$z^\top = \left[\frac{\lambda_1\eta_1 + \eta_2}{\lambda_1 - \lambda_2}, \;\; \frac{\lambda_2\eta_1 + \eta_2}{\lambda_1 - \lambda_2}, \;\; \eta_3 + \frac{(\tau+1)\eta_1^2}{2(\lambda_1 - \lambda_2)} \right]. \tag{11}$$

Theorem 3 *Consider system (8-9) 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 $\hat{\eta} = (\hat{\eta}_1, \hat{\eta}_2, \hat{\eta}_3)^\top$:*

$$\frac{\mathrm{d}\hat{\eta}}{\mathrm{d}t} = \begin{bmatrix} l_1 & 1 & 0 \\ l_2 & 0 & 0 \\ 0 & 0 & \lambda_3 \end{bmatrix} \hat{\eta} + \begin{bmatrix} \lambda_1 + \lambda_2 - l_1 \\ -\lambda_1\lambda_2 - l_2 \\ 0 \end{bmatrix} \eta_1^m + \begin{bmatrix} 0 \\ -(\lambda_1 - \lambda_2)\eta_1^m\hat{\eta}_3 - (1/2)(\tau+1)(\eta_1^m)^3 \\ K_1(\tau)(\eta_1^m)^2 \end{bmatrix}, \tag{12}$$

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 (12) is a global exponential observer for system (8)-(9).

Remark 1 *One can easily see that the right-hand side of the observer (12) can be represented in the form required by Definition 1, i.e., as a copy of the system plus a synchronizing connection term.*

Remark 2 *The generalized Lorenz system as well as the generalized Lorenz canonical form were already used for chaos synchronization in [33], which however uses linear coupling only. As a consequence, a rigorous proof of the error convergence was possible only in a very restricted case when $a_{22} < 0$ (see (5)). Yet, for the chaotic Chen system, $a_{22} > 0$. Notice that for the case of $a_{22} < 0$, the synchronization problem is trivial and can be achieved in the same way as that for the Lorenz system (see [42]). On the contrary, the majority of chaotic behaviors are presented with $a_{22} \geq 0$ (see [10]), so does the Chen system. For these common and important cases of $a_{22} \geq 0$, in [33] an ad hoc requirement on the magnitude of the driving signal was introduced, which may only be checked experimentally for a specifically given system. Although Assertion 3 of [10] proves the boundedness of the GLS behavior for the case of $a_{22} \geq 0$, no explicit theoretical estimates on the attractor size were provided. The approach presented here provides the global exponential convergence of the synchronization error for any transmitter behavior and for all values of the system parameters; therefore, this approach is very general.*

The following proposition analyzes the influence of mismatching the parameter τ, where system (8)-(9) with chaotic behavior is considered.

Proposition 3 *System (12), with $\eta_1 = \eta_1^m$, $\tau = \tau_{sl}$ and system (8)-(9) with $\tau = \tau_{mast}$ satisfy the following property: For $i = 1, 2, 3$ and for sufficiently small $|\tau_{mast} - \tau_{sl}|$,*

$$\overline{\lim}_{t\to\infty} |\hat{\eta}_i(t) - \eta_i(t)| \leq C_i^{up}(l_1, l_2)|\tau_{mast} - \tau_{sl}|,$$

where $C_i^{up}(l_1, l_2) > 0$, $i = 1, 2$, are some parameters converging to zero if $(1/2)(l_1 \pm \sqrt{l_1^2 + 4l_2}) \to -\infty$, while $C_3^{up}(l_1, l_2) > 0$ does not depend on $l_{1,2}$. For all values of $l_{1,2}$, it holds that

$$\frac{\mathrm{d}(\eta_3 - \hat{\eta}_3)}{\mathrm{d}t} = \lambda_3(\eta_3 - \hat{\eta}_3) + K_1(\tau_{mast} - \tau_{sl})\eta_1^2, \tag{13}$$

where K_1 is given in (9).

Remark 3 *A study similar to Proposition 3 may be carried out with respect to other system parameters and biased output measurements. Anti-robust security can also be obtained, thanks to the special structure of the observer used, i.e., the third component is detectable but unobservable, which leads the third component of the error to be independent of the gains $l_{1,2}$, evolving as the chaotic signal η_1 passes through a simple linear filter. This means that wrongly synchronized system creates a signal qualitatively similar to the correct one but no hint for the intruder is provided. Moreover, Proposition 1 is not applicable to system (8)-(9) since the last equality in (4) together with $C^\top = (1, 0, 0)$ and S being nonsingular gives $\mathrm{rank}B = 1$. The latter property does not provide enough freedom to incorporate all the influence of τ in (8)-(9). Notice also that for $\eta_1 = 0$, there is a singularity preventing further transforming the observer canonical form (8)-(9) into an observability form, where the latter enables the use of Proposition 2 or Proposition 1 with B having rank equal to 1.*

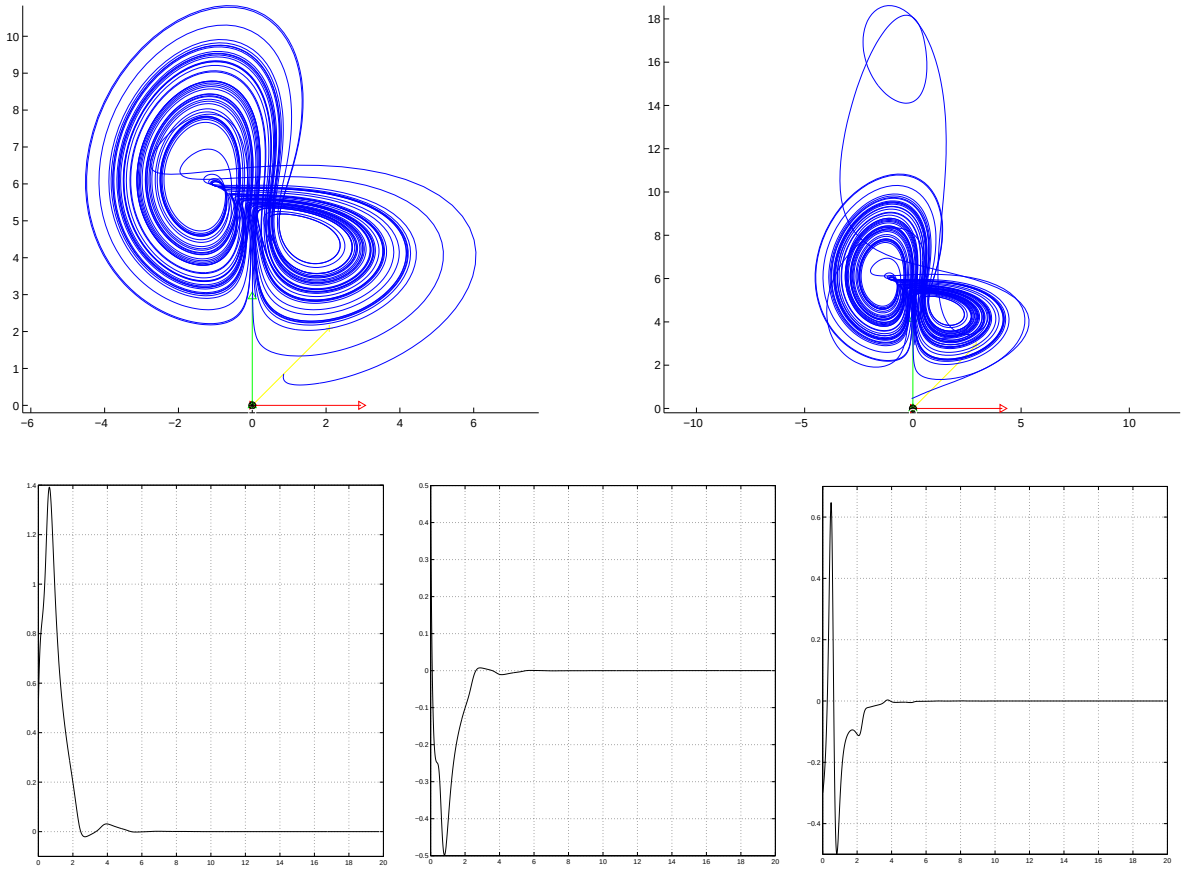


Figure 2: Synchronization of the generalized Lorenz system for the case with $\lambda_1 = 8$, $\lambda_2 = -16$, $\lambda_3 = -1$ and $\tau = 0.5$. From left to right: the transmitter oscillator and the receiver oscillator; bottom: the first, second, and third error components between them.

Clearly, the above properties do not provide a full scale of security for the suggested synchronization, even in the rather simplified Definition 1. Nevertheless, they exclude a great deal of possible cipher breaking schemes, thereby making the GLS class more attractive than most, if not all, existing ones for secure encryption applications.

Based on the facts described in the above remark, one may formulate the following conjecture.

Conjecture 1 *Generalized Lorenz system allows secure synchronization.*

The generalized Lorenz system (GLS) has been used in [16, 14, 15] to implement the ACSK method. In these works, a thorough investigation of speeds of synchronization and de-synchronization was performed. Based on it, the generalized Lorenz system provides experimental algorithm that is able to provide realistic, though still not optimal, way how to encrypt digital data using continuous-time chaotic systems.

5 Conclusions

The aim of the present lecture was to demonstrate concept of the secure synchronization of chaotic systems with application to secure encryption of sensitive data. Despite numerous possible encryption schemes, all of them are based on the possibility to synchronize two chaotic systems, moreover, such a synchronization should be available to authorized persons only. The particular class of chaotic systems enabling synchronization has been then suggested and the security of that synchronization was investigated. The system in question, called as the generalized Lorenz system, appears to have a great potential to be used in various encryption schemes. As an example, the recent implementation of ACSK scheme based on the generalized Lorenz system was mentioned.

References

[1] Agiza, H.N. and M.T. Yassen: "Synchronization of Rössler and Chen chaotic dynamical systems using active control", *Phys. Lett. A*, vol. 278, 2000, pp. 191-197.

[2] Alvarez, J., H. Puebla and I. Cervantes: "Stability of observer-based chaotic communitcation for a class of Lur'e systems", *Int. J. of Bifur. Chaos*, vol. 7, 2002, pp. 1605-1618.

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

[4] Anderson, R.: "Chaos and random numbers", *Cryptologia*, vol. XVI, 1992, no. 3, p. 226.

[5] Biham, E.: "Cryptanalysis of the chaotic-map cryptosystem suggested at EUROCRYPT91", in *Advances in Cryptology - EUROCRYPT91*, D. W. Davies (Ed.), Springer-Verlag, New York, vol. 547, 1991, pp. 532-534.

[6] Blekman, I.I., A.L. Fradkov, H. Nijmeijer and A.Y. Pogromsky: "On self-synchronization and controlled synchronization", *Systems and Control Letters*, vol. 31, 1997, pp. 299-305.

[7] Carroll, J.M., J. Verhagen, and P. T. Wong, "Chaos in crytography: The escape from the strange attractor", *Cryptologia*, vol. XVI, 1992, pp. 52-71.

[8] Chen, G. and X. Dong, *From Chaos to Order: Methodologies, Perspectives, and Applications*, World Scientific Pub. Co., Singapore 1998.

[9] Chen, G. and T. Ueta, "Yet another chaotic attractor", *Int. J. of Bifur. Chaos*, 9 (1999), pp. 1465-1466.

[10] Čelikovský S. and A. Vaněček: "Bilinear systems and chaos", *Kybernetika*, vol. 30, 1994, pp. 403-424.

[11] Čelikovský, S. and G. Chen: "On a generalized Lorenz canonical form of chaotic systems" *Int. J. of Bifur. Chaos*, 12, 2002, 1789-1812.

[12] Čelikovský, S. and Chen, G.: "Secure synchronization of chaotic systems from a nonlinear observer approach", *IEEE Trans. Aut. Contr.* vol. 50, 2005, pp. 76-82.

[13] Čelikovský S. and G. Chen: "On the generalized Lorenz canonical form, *Chaos Solitons & Fractals*, vol.26, 2005, pp. 1271-1276.

[14] Čelikovský S., V. Lynnyk and Šebek M.: "Anti-synchronization chaos shift keying method based on generalized Lorenz system", *Proceedings of the 1st IFAC Conference on Analysis and Control of Chaotic Systems (CHAOS '06)*, Reims, June 2006, pp. 333-338.

[15] Čelikovský S., V. Lynnyk: "Observer-based chaos synchronization and its application to multi-valued alphabet chaos shift keying secure encryption", *Proceedings of the 6th Asian Control Conference, ASCC 2006*, Bali, Indonesia, July 2006, pp. 52-57.

[16] Čelikovský S., V. Lynnyk, M. Šebek: "Observer-based chaos synchronization in the generalized chaotic Lorenz systems and its application to secure encryption", *Proceedings of the 45th IEEE Conference on Decision and Control*, San Diego, CA, USA, December 2007, pp. 3783-3788.

[17] Dachselt, F. and W. Schwartz. "Chaos and cryptography", *IEEE Trans. Circ. Syst. I: Fund. Th. and Appl.*, vol. 48, 2001, pp. 1498-1509.

[18] Dedieu H., Kennedy M.P., Hasler M.: "Chaos shift keying: modulation and demodulation of a chaotic carrier using self-synchronizing Chua's circuit", *IEEE Transactions on Circuits and System Part 2*, vol. 40, 1993, pp. 634-642.

[19] Feldmann, U., M. Hasler, and W. Schwarz: "Communication by chaotic signals: The inverse system approach", *Int. J. Circuit Theory Appl.*, vol. 24, 1996, pp. 551-579.

[20] Fradkov, A.L., H. Nijmeijer and A.Yu. Pogromsky: "Adaptive observer based synhronization", in: G. Chen (Ed.), *Controlling Chaos and Bifurcations in Engineering Systems*, CRC Press, Boca Raton, FL, 1999, pp. 417-435.

[21] Frey, D.R.: "Chaotic digital encoding: An approch to secure communication", *IEEE Trans. Circuits Syst. II*, vol. 40, 1993, pp. 660-666.

[22] Gauthier, J.P., H. Hammouri and S. Orthman, "Simple observer for nonlinear systems application to bioreactors," *IEEE Trans. Aut. Contr.*, 37 (1992), 875-880.

[23] Grassi, G. and S. Mascolo: "Synchronization of high-order oscillators by observer design with application to hyperchaos-based cryptography," *Int. J. of Circ. Theory and Appl.*, vol. 27, 1999, pp. 543-553.

[24] Gubanov D., A. Dmitriev, A. Panas and S. Starkov: Steshenko V. "Generators of chaos in integrated execution", *CHIP News*, vol. 12, 1999, pp. 9-14.

[25] Habutsu, T., Y. Nishio, I. Sasase, and S. Mori: "A secret key cryptosystem by iterating a chaotic map", in *Advances in Cryptology - EUROCRYPT 91*, D. W. Davies, Ed., Springer-Verlag, New York 1991, vol. 547, pp. 127-140.

[26] He, Z., K. Li, L. Yang, and Y. Shi: “A robust digital secure communication scheme based on sporadic coupling chaos synchronization”, *IEEE Trans. Circuits Syst. I*, vol. 47, 2000, pp. 397-403.

[27] Itoh, M. and L.O. Chua: “Reconstruction and synchronization of hyperchaotic circuits via one state variable”, *Int. J. of Bifur. Chaos*, vol. 12, 2002, pp. 2069-2085.

[28] Kelber, K., T. Falk, M. Götz, W. Schwarz, and T. Kilias: “Discrete-time chaotic coders for information encryptionPart 2: Continuous- and discrete- value realization”, *Proc. Workshop Nonlinear Dynamics of Electronic Systems (NDES96)*, 1996, pp. 27-32.

[29] Khalil, H.K: *Nonlinear Systems - Third Edition*. Prentice Hall, London 2002.

[30] Kocarev, L., G. Jakimoski, T. Stojanovski, and U. Parlitz: “From chaotic maps to encryption systems”, in *Proc. Int. Symp. Circuits and Systems (ISCAS98)*, vol. IV, 1998, pp. 514-517.

[31] Kocarev L., Chaos-Based Cryptography: A Brief Overview, *IEEE Circuits and Systems Magazine,* Vol.1, No.3, 6-21.

[32] Lau, F.C.M and C.K.Tse: *Chaos-based digital communication systems*, Springer Verlag, Heidelberg 2003.

[33] Lian, K. and P. Liu: “Synchronization with message embedded for generalized Lorenz chaotic circuits and its error analysis”, *IEEE Trans. Circ. Syst.–I*, vol. 47, 2000, pp. 1418-1424.

[34] Leuciuc, A. and V. Grigoras: “Multi-parameter chaos modulation of discrete- time filters”, *Proc.Workshop Nonlinear Dynamics of Electronic Systems (NDES97)*, 1997, pp. 81-86.

[35] Leuciuc, A.: “Information transmission using chaotic discrete-time filter”, *IEEE Trans. Circuits Syst. I*, vol. 47, 2000, pp. 82-88.

[36] Lü, J., G. Chen, D. Cheng and S. Čelikovský: “Bridge the gap between the Lorenz system and the Chen system” *Int. J. of Bifur. Chaos*, 12, 2002, pp. 2917-2926.

[37] Marino, P. and P. Tomei: *Nonlinear Control Design: Geometric, Adaptive and Robust*, Prentice-Hall, London 1991.

[38] Matthews, R.: “On the derivation of a “chaotic” encryption algorithm”, *Cryptologia*, vol. XIII, 1989, pp. 29-41.

[39] Maurer, U.M.: “New approaches to the design of self-synchronizing stream ciphers”, in *Advances in CryptologyEUROCRYPT91 - Lecture Notes in Computer Science, vol. 547*, D. W. Davies, Ed., Springer-Verlag, New York, 1991, pp. 458-471.

[40] Mitchell, D.W.: “Nonlinear key generators”, *Cryptologia*, vol. XIV, 1990, pp. 350-354.

[41] Nijmeijer, H. and A.J. van der Shaft: *Nonlinear Dynamical Control Systems*, Springer-Verlag, New York 1990.

[42] Nijmeijer, H., “A dynamical control view on synchronization”, *Physica D*, vol. 154, 2001, pp. 219-228.

[43] Parlitz U., L.O. Chua, L Kocarev, K.S. Halle and Shang A.: "Transmission of digital signals by chaotic synchronization", *Int. J. of Bifur. Chaos*, vol. 2, 1992, pp. 973-977.

[44] Papadimitriou, S., G. Pavlides, A. Bezerianos, and T. Bountis: "Chaotic systems of difference equations for real-time encryption", *Proc. Workshop Nonlinear Signal and Image Processing (NSIP95)*, 1995, pp. 145-149.

[45] Papadimitriou, S., A. Bezerianos, and T. Bountis: "Secure communication with chaotic systems of difference equations", *IEEE Trans. Comput.*, vol. 46, 1997, p. 27.

[46] Pecora, L. and T. Carrol: "Synchronization in chaotic systems", *Phys. Rev. Lett.*, vol. 64, 1990, pp. 821-824.

[47] Pogromsky, A., G. Santoboni and H. Nijmeijer,: "Partial Synchronization: from symmetry towards stability", *Physica D*, vol. 172, 2002, pp. 65-87.

[48] Roskin, K.M. and J. B. Casper: *From Chaos to Cryptography.* [Online]. Available: http://xcrypt.theory.org/.

[49] Rueppel, R.A.: "Stream ciphers", in *Contemporary Cryptology*, G. J. Simmons, Ed., Piscataway, NJ: IEEE Press, 1992, ch. 2, pp. 65-134.

[50] Santoboni, G., A.Y. Pogromsky and H. Nijmeijer: "An observer for phase synchronization of chaos", *Phys. Lett. A*, vol. 291, 2001, pp. 265-273.

[51] Santoboni, G., A.Y. Pogromsky and H. Nijmeijer: "Partial observer and partial synchronization", *Int. J. of Bifur. Chaos*, vol. 13, 2003, pp. 453-458.

[52] Shilnikov, A.L., L.P. Shilnikov, and D.V. Turaev,: "Normal forms and Lorenz attractors", *Int. J. of Bifur. Chaos*, vol. 3, 1993, pp. 1123-1139.

[53] Solak, E., Ö. Morgül and U. Ersoy: "Observer-based control of a class of chaotic systems," *Phys. Lett. A*, vol. 279, 2001, pp. 47-55.

[54] Ueta, T. and G. Chen: "Bifurcation analysis of Chen's equation", *Int. J. of Bifur. Chaos*, vol. 10, 2000, pp. 1917-1931.

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

[56] Wang, X.: "Chen's attractor – A new chaotic attractor" (in Chinese), *Control Theory and Applications*, vol. 16, 1999, p. 779.

[57] Wheeler, D.D.: "Problems with chaotic cryptosystems", *Cryptologia*, vol. XIII,1989, pp. 243-250.

[58] Wiggins, S.: *Global Bifurcation and Chaos: Analytical Methods*, Springer-Verlag, New York 1988.

[59] Wu, C.W. and L. O. Chua: "A simple way to synchronize chaotic systems with applications to secure communication systems", *Int. J. Bifurcation Chaos*, vol. 3, 1993, pp. 1619-1627.

[60] Yang, T., C. W. Wu, and L. O. Chua: "Cryptography based on chaotic systems", *IEEE Trans. Circuits Syst. I*, vol. 44, 1997, pp. 469-472.

[61] Zhou, H. and X. T. Ling: “Problems with the chaotic inverse system encrytion approach”, *IEEE Trans. Circuits Syst. I*, vol. 44, 1997, pp. 268-271.

[62] Zhou, T., G. Chen and S. Čelikovský: “Ši’lnikov Chaos in the Generalized Lorenz Canonical Form of Dynamical Systems”, *Nonlinear Dynamics*, 2005, vol. 39, pp. 319-334.

RNDr. Sergej Čelikovský, CSc.

Curriculum vitae

1984: MSc. from Faculty of Numerical Mathematics and Cybernetics of the Moscow State University, Department of Optimal Control.

1985: RNDr. degree (Rerum Naturalium Doctoris) from the Mathematical and Physical Faculty of Charles University in Prague.

1989: CSc. degree (Candidate of Sciences - corresponds to Ph.D degree) from the Institute of Information Theory and Automation of the Czechoslovak Academy of Sciences.

1989-2003: Research fellow and, later on, **Senior research fellow** in the Department of Control Theory of Institute of Information Theory and Automation of the Academy of Sciences of the Czech Republic.

1998: Half year position of research associate at the Department of Mechanical and Automation Engineering of the Chinese University of Hong Kong.

1998-2000: On the leave in CINVESTAV-IPN, Unidad Guadalajara, Mexico as Level 3A visiting professor.

2001-now: Associate member of the Centre for Chaos and Synchronization at the City University of Hong Kong.

2003-now: Chief research fellow in the Institute of Information Theory and Automation of the Academy of Sciences of the Czech Republic.

2003-now: Research fellow and, later on, assistant professor at Department of Control Engineering, Faculty of Electrical Engineering, Czech Technical University in Prague.

2004-now: Head of Department of Control Theory Institute of Information Theory and Automation of the Academy of Sciences of the Czech Republic.

Technical societies and journals: Secretary of the Czech National Committee for Automation and IFAC (International Federation of Automatic Control). Senior Member of the Institute of Electrical and Electronics Engineers, Inc. (IEEE), Member of IFAC TC on Nonlinear Systems and IFAC TC on Robust Control. Member of the Steering Committee of the ERCIM Working Group Control and System Theory.

Editorial boards: Associate Editor of *IEEE Transaction on Automatic Control*; Member of Editorial Board of *Kybernetika*.

Conferences: Member of the Organizing Committee of the IFAC World Congress, Prague 2006. Sub-area Chair of the International Programme Committee of the IFAC NOLCOS (Nonlinear Control Symposium) 2007.

Research expertise: Nonlinear systems, chaotic systems control and synchronization, numerical methods, stability and stabilization, observers and filtering, robotics, underactuated mechanical systems control.

Publications summary: 37 papers in international journals, over 50 papers in international conference proceeding, over 140 SCI citations.