***REVIEWS OF TOPICAL PROBLEMS***

PACS numbers: **05.45.–a**, 05.45.Pq, 05.45.Tp, 05.45.Vx, 05.45.Xt

# On the use of chaotic synchronization for secure communication

A A Koronovskii, O I Moskalenko, A E Hramov

DOI: 10.3367/UFNe.0179.200912c.1281

## Contents

Abstract. **Research on the secure communication applications of chaotic synchronization is reviewed. A number of secure communication methods and devices using different types of synchronous behavior are examined. For the purpose of comparing existing methods, quantitative characteristics of operating capacity of various schemes are introduced and estimated. An extremely noise-stable secure information transmission method, based on the phenomenon of generalized chaos synchronization, is proposed. All of the methods considered are systematically checked for efficiency for the first time by numerically simulating unidirectionally coupled chaotic Rössler systems selected for transmitting and receiving oscillators. The key advantages and disadvantages of secure information transmission schemes using synchronized chaotic oscillations are discussed. The experimental data gathered in this field are also reviewed.**

**A A Koronovskii, O I Moskalenko, A E Hramov** Faculty of Nonlinear Processes, N G Chernyshevsky Saratov State University,
ul. Astrakhanskaya 83, 410012 Saratov, Russian Federation
Tel. (7-8452) 51 21 11, (7-8452) 51 42 94
Fax (+7-8452) 52 38 64, (7-8452) 52 38 64
E-mail: moskalenko@nonlin.sgu.ru,
aeh@nonlin.sgu.ru, hramov@gmail.com

Received 27 February 2009, revised 10 August 2009
*Uspekhi Fizicheskikh Nauk* **179** (12) 1281 – 1310 (2009)
DOI: 10.3367/UFNr.0179.200912c.1281
Translated by Yu V Morozov; edited by A Radzig

## 1. Introduction

Synchronization of auto-oscillatory processes is a fundamental nonlinear phenomenon that has been attracting the close attention of researchers for a few centuries [2 – 16], ever since C Huygens first described it for the example of coupled mechanical systems (pendulum clock) [1]. In the last few decades, studies in this area have been focused on synchronization of self-sustained chaotic oscillations in conjunction with increasingly greater interest, in nonlinear physics, in the problem of deterministic chaos and various applications of the chaos theory [12, 13, 17 – 23]. The development of dynamical chaos theory naturally led to investigations into chaotic synchronization, which stems from both its great fundamental importance [11, 13, 14] and wide practical implementations for secure information transmission [24 – 35], in biological [36 – 43], physiological [44 – 54], and chemical problems [55 – 59], for chaos management, including microwave electronic systems [67 – 70], and so forth.

Recently, researchers have given increasingly more attention to living systems [46, 72, 73], besides radiophysical models and systems for which the most essential data were obtained (see reviews [11, 71]). Worthy of note in this context are studies of the effect of external stimuli on brain electrical activity (EEG) [74, 75], the interplay between rhythmic activities of respiratory and cardiovascular systems [45, 47, 53], dynamic synchronization of neuronal ensembles in different brain regions of epileptic patients [76, 77], etc. Very important results of these studies find progressively wider application in physiology, medicine, and experimental data

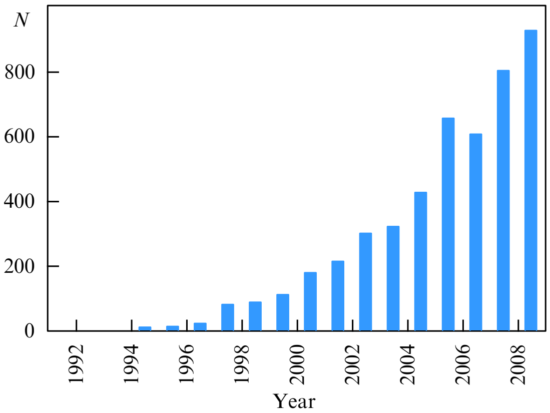

**Figure 1.** Number of citations of publications devoted to employment of chaotic synchronization in information telecommunication systems in major peer-reviewed journals for different years (from *ISI Web of Knowledge* as of December 2008).

processing. However, the possibilities of employing chaotic synchronization are not confined to physiology and medicine. One of the most interesting and rapidly developing areas of research is the application of chaotic synchronization to the solution of telecommunication problems, first and foremost for designing systems of secure information transmission. At the same time, there are only a few reviews concerned with the application of chaotic synchronization in information telecommunication systems. Those available to date include Refs [23, 78], but the information they contain is far from complete, bearing in mind the rapid development of relevant research. The number of publications on these issues referred to in *ISI Web of Knowledge* have increased 50-fold during the past decade (see, for instance, Refs [79 – 92]), and their citation index has grown almost exponentially (Fig. 1). Finally, it is vital to note that this process was paralleled by transition from theoretical consideration of the problem to designing practically applicable devices allowing for chaos synchronization-based secure information transmission over tens of kilometers using previously created telecommunication systems [93]. The aforesaid illustrates the importance of issues being considered and the necessity of a review summarizing, generalizing and comparing the currently available data.

The majority of secure communication methods based on chaos synchronization use primarily complete chaotic synchronization regimes [94, 95] that imply a close identity of oscillators at opposite ends of the communication channel. The discovery and extensive studies of other types of synchronous behaviour of coupled chaotic systems (e.g., phase synchronization [96], generalized synchronization [97], lag synchronization [98], noise-induced synchronization [99 – 104]) made possible their employment for improving secure communication techniques and promoting the development of dynamical chaos-based information telecommunication systems.

The review outline is as follows. Section 2 describes in brief various types of synchronous behavior of coupled chaotic systems providing a basis for the creation of secure information transmission schemes (first and foremost complete, phase, and generalized chaotic synchronization regimes). Complete chaotic synchronization-based secure communication techniques are considered in Section 3. The use of other types of synchronous behavior for secure communication and methods of information transmission using simultaneously a few types of the synchronous behavior are discussed in Section 4. Section 5 contains the description of an extremely noise-stable secure communication method free of drawbacks inherent in all known schemes and devices for the same purpose. Section 6 presents results of comparative analysis of operating capacities of the secure communication techniques reviewed in Sections 3 – 5; these quantitative characteristics are used to assess the key advantages of the extremely noise-stable scheme over other methods. Section 7 describes the results of experimental realization of information transmission schemes based on chaotic synchronization in the radio frequency band, microwave and optical ranges. Section 8 presents a summary discussion and conclusions.

It should be noted that some secure communication methods considered in the present review are suitable for the transmission of digital signals alone, while others can be used to transmit both analog and digital signals. In order to achieve generality and facilitate comparison of all these methods, we consider below only digital signals as information ones.[1] Notice also that consideration is confined to chaotic synchronization-based information transmission techniques, in strict agreement with the title of the review. These are steganographic means for maintaining information security that, unlike cryptographic ones, conceal the fact of transmission rather than hide the content or nature of a communication.

Basic advantages of chaotic synchronization-based techniques over traditional ones [e.g., least significant bit (LSB) method, echo-method, extended spectrum method] are the considerably enhanced robustness against noises and distortions in the communication channel and the high information transmission rate [105]. Moreover, the utilization of chaotic synchronization is paramount for increasing confidentiality of data transfer. Alternative approaches to secure information transmission using dynamic chaos-based methods have also been described (see the monograph by A S Dmitriev and A I Panas [23], extensively cited as a classical work). They are exemplified by direct chaotic communication systems based on direct generation of information-carrying chaotic oscillations, e.g., in the microwave range, and their modulation with information signals. Such methods are relatively easy to realize, and they permit reaching a data transmission rate as high as 200 Mb $s^{-1}$. However, the degree of confidentiality in chaos synchronization-based schemes is much higher.

Despite a variety of publications on the application of chaotic synchronization in information telecommunication systems (see Refs [106 – 110]), it is safe to say that the basis of most information transmission techniques is constituted by the very first well-known secure communication methods employing the phenomenon of complete chaotic synchronization. One of the first such methods was proposed by Pecora and Carroll [95]. They laid the foundation for more sophisticated techniques that, nonetheless, inherited certain drawbacks from their prototypes. For this reason, we shall consider not only the early methods but also those most different from them.

The influence of noise and distortion of signals on the performance of transmitting systems is a major concern in the context of information transfer. Noises are known to

[1] To recall, analog signals can be transformed into digital ones; this justifies such detailed consideration of the latter and permits avoiding the loss of generality.

invariably affect the dynamics of these systems and to considerably change both the behaviour and the efficiency of chaos synchronization-based schemes [111 – 122]. Nonlinear distortions also impair the performance of such schemes [23]. For all that, chaos synchronization-based information transmission systems are usually considered neglecting noises and distortions, which accounts for many unresolved problems with their practical application and efficiency. They are considered at greater length in Section 6.

## 2. Main types of chaotic synchronization in coupled dynamical systems

As mentioned in the Introduction, the main types of chaotic synchronization underlying modern communication systems are complete, phase, and generalized synchronization regimes. In what follows, we briefly describe these types of synchronous behavior to present an integrated picture.

*Complete synchronization* regime [94, 95] implies exact correspondence between state vectors of interacting (unidirectionally or reciprocally coupled) systems: $\mathbf{x}(t) \equiv \mathbf{u}(t)$; therefore, this regime is feasible only for their identity in terms of control parameters. When these parameters are slightly different, *lag synchronization* may occur [98, 123], in which the interacting systems undergo almost identical oscillations but shifted over a certain time interval $\tau$, i.e., $\mathbf{x}(t) \approx \mathbf{u}(t+\tau)$. As the coupling strength between the slightly detuned oscillators increases, the time shift $\tau$ tends to zero and the lag synchronization regime tends toward complete chaotic synchronization. The latter is rather frequently diagnosed by direct comparison of state vectors $\mathbf{x}(t)$ and $\mathbf{u}(\mathbf{t})$ of interacting systems and calculation of synchronization error [124]:

$$\langle e \rangle = \int_0^{\infty} \| \mathbf{x}(t) - \mathbf{u}(t) \| \, \mathrm{d}t \,. \tag{1}$$

It should be emphasized that complete chaotic synchronization is not infrequently considered in the literature along with synchronization of chaotic systems obtained as a result of the decomposition [94] of an auto-oscillatory system or the so-called 'chaotic synchronous response' [125]. Decomposition turns the auto-oscillatory system into a circular structure, with the subsystems making up an integral feedback loop. At the next stage, two identical systems resulting from similar decomposition are used, with one remaining unaltered (auto-oscillatory drive or active system) and the other (response or passive system) having its feedback loop broken. If a signal from the output of one of the subsystems of the drive system is fed to the input of another subsystem of the response system, the difference between input and output signals of the response system tends to vanish under certain conditions, i.e., complete synchronization between the states of the drive and response systems is achieved [23].

*Generalized synchronization*, introduced in the consideration of a system of two unidirectionally coupled chaotic oscillators, drive $\mathbf{x}(t)$ and response $\mathbf{u}(t)$, means that the completion of the transient process is followed by the establishment of a functional dependence between their states: $\mathbf{u}(t) = F[\mathbf{x}(t)]$ [97]. The form of this dependence $F[\cdot]$ can be rather complicated and the procedure for finding it quite untrivial [126].

A few procedures have been proposed for the diagnostics of generalized synchronization regime between chaotic oscillators, such as the method of nearest neighbors [97, 127], calculation of conditional Lyapunov exponents [95, 128], and the frequently used easy-to-realize auxiliary system method [129].

The essence of the last method is as follows. Here, one considers a response system $\mathbf{u}(t)$ along with an identical auxiliary system $\mathbf{v}(t)$. Initial conditions for the auxiliary system $\mathbf{v}(t_0)$ are chosen to differ from those for the response system $\mathbf{u}(t_0)$, but to remain within the basin of attraction of the same attractor (in practical terms, this means a small mismatch between the initial conditions, which is realized automatically due to the presence of fluctuations). In the absence of the regime of generalized synchronization between the interacting systems, the state vectors $\mathbf{u}(t)$ and $\mathbf{v}(t)$ of the response and auxiliary systems, respectively, are different, even if they belong to one and the same chaotic attractor. In the regime of generalized synchronization, the transient process results in identical states of the response and auxiliary systems, $\mathbf{u}(t) \equiv \mathbf{v}(t)$, due to fulfillment of the relation $\mathbf{u}(t) = F[\mathbf{x}(t)]$ and, accordingly, $\mathbf{v}(t) = F[\mathbf{x}(t)]$. Thus, equivalence of states of the response and auxiliary systems after completion of the transient process is a criterion for the occurrence of generalized synchronization between the drive and the response oscillators.

Analysis of the generalized synchronization regime is also possible by calculating conditional Lyapunov exponents [95, 128]. Denoting the dimensions of phase spaces of drive and response systems by $N_{\mathrm{d}}$ and $N_{\mathrm{r}}$, respectively, one can characterize the behavior of unidirectionally coupled systems utilizing a set of Lyapunov exponents $\lambda_1 \geqslant \lambda_2 \geqslant \ldots \geqslant \lambda_{N_{\mathrm{d}}+N_{\mathrm{r}}}$. The behavior of the drive system being unrelated to the state of the response oscillator, the spectrum of Lyapunov exponents may be divided into two parts: Lyapunov exponents of the drive system, $\lambda_1^{\mathrm{d}} \geqslant \ldots \geqslant \lambda_{N_{\mathrm{d}}}^{\mathrm{d}}$, and conditional Lyapunov exponents $\lambda_1^{\mathrm{r}} \geqslant \ldots \geqslant \lambda_{N_{\mathrm{r}}}^{\mathrm{r}}$. The criterion for the occurrence of generalized synchronization in unidirectionally coupled dynamical systems [95, 126] is the negativeness of the senior conditional Lyapunov exponent $\lambda_1^{\mathrm{r}}$. Notice that complete synchronization and lag synchronization regimes for unidirectionally coupled chaotic oscillators are peculiar cases of the generalized synchronization regime [126].

*Phase synchronization* [96, 130] means the capture of chaotic signal phases, while the amplitudes of these signals remain unrelated and look chaotic. The concept of chaotic phase synchronization is based on the notion of instantaneous phase $\phi(t)$ of a chaotic signal [96, 130 – 132]. There is no universal method for the introduction of a chaotic signal phase that would yield correct results for all dynamical systems. Conversely, there are several methods for the purpose applicable to systems with a sufficiently simple topology of the chaotic attractor, referred to in the literature as 'systems with a well-defined phase' or 'systems with a phase-coherent attractor' [13, 133]. The chaotic attractor of these systems should be such that a projection of the phase trajectory onto a certain plane $(x, y)$ of states rotates continuously about a certain center without crossing or rounding it. Then, instantaneous phase $\phi(t)$ of the chaotic signal can be introduced into the consideration in one of the following ways: as an angle in the polar system of coordinates [98, 134], by the Gilbert transform of signal temporal realization [96, 131], or using the surface of the Poincaré section [96, 131]. However, for systems with an ill-defined phase (see, e.g., Refs [133, 135]), these methods do not work

[136]. Nevertheless, phase synchronization of such systems can be detected in certain cases by indirect observations [134, 137] and measurements [138, 139].

Phase synchronization arises when the difference between instantaneous phases of chaotic signals $\mathbf{x}_{1,2}(t)$, introduced by one of the above methods, is limited in time:

$$\left|\phi_1(t) - \phi_2(t)\right| < \text{const}\,. \qquad (2)$$

It is worth mentioning that the notion of 'phase synchronization' can be generalized by introducing into the consideration a set of time scales $s$ and their associated phases $\phi_s(t)$ of the chaotic signal using a continuous wavelet transform with a complex basis [140, 141]. Given a range (or a set of ranges) of time scales $s_{\rm m} < s < s_{\rm b}$, with the phase capture condition analogous to Eqn (2) being fulfilled for each of them, and given further the nonzero fraction of the wavelet spectrum energy for this range, time scales $s$ prove synchronized and chaotic oscillators are in the time scale synchronization regime. In certain cases (see, for instance, Ref. [142]), synchronization of even a single time scale suggests the occurrence of phase synchronization. However, the case of systems with a phase-incoherent attractor, where phase synchronization cannot be diagnosed by traditional methods, is described as *time scale synchronization* [69, 77, 140, 143).

Also worthy of note is that time scale synchronization makes it possible to consider all the above types of chaotic synchronization on a common basis. The character of the synchronous regime is determined in this case only by the range of synchronous time scales [140, 141, 144].

## 3. Secure communication techniques based on complete chaotic synchronization

Let us now move to secure communication techniques based on chaotic synchronization, starting from the complete synchronization regime, because the majority of the known methods and devices lean upon this type of synchronous behavior.

The use of complete chaotic synchronization for secure information transmission implies the presence of at least two unidirectionally coupled identical chaotic oscillators. There are many methods based on this principle, viz. chaotic masking [25], chaotic regime switching [145], the nonlinear mixing of an information signal with a chaotic one [146], the modulation of control parameters of a transmitting oscillator with a valid information signal [147], etc. These methods constitute the basis of many secure communication techniques; hence, the importance of considering their basic principles, expounded at greater length below.

### 3.1 Chaotic masking

Chaotic masking is one of the first and simplest techniques for transmitting information in a secure fashion [25]. A schematic diagram of this method is shown in Fig. 2. The information signal $m(t)$ is combined in the summator with a carrier generated by the chaotic system $\mathbf{x}(t)$ for transmission through the communication channel. The received signal causes complete chaotic synchronization of the chaotic oscillator $\mathbf{u}(t)$ in the receiver; as a result, the dynamics of the receiving oscillator become identical to that of the transmitting one. The detected signal $\tilde{m}(t)$ is produced after passing through the subtractor as the difference between the received signal and the synchronous response of the chaos oscillator in the receiver (see, e.g., Refs [23, 25]).

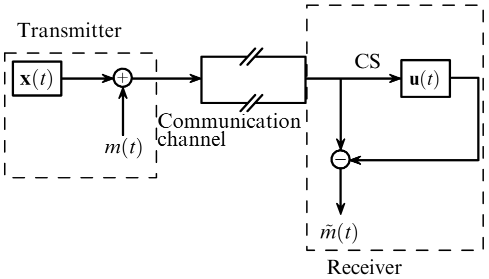

**Figure 2.** Schematic of a chaotically masked secure communication system (CS — complete chaotic synchronization).

Such a scheme of secure communication operates rather efficiently (in that it ensures high-quality transmission of information and its detection at the outlet) in the absence of noise in the channel, when the power of the signal generated in the transmitting system is 35 – 65 dB higher than that of the information signal [148]. Given a noisy channel, the quality of transmitted information worsens considerably; this accounts for the high signal-to-noise ratio at which the system remains operative. Moreover, the introduction of a parameter mismatch between identical chaotic oscillators (located at opposite ends of the communication channel) results in the appearance of additional desynchronization noises at the outlet and makes transmission difficult to realize [23]. Also, there is the problem of confidentiality in data transmission.[2] Despite the low level of the information signal compared with that of the carrier, certain methods and approaches allow restoring the initial chaotic signal from the signal transmitted over the communication channel and thereby extracting the desired information [149 – 151].

All these drawbacks make secure communication systems based on chaotic masking impracticable.

### 3.2 Chaotic regime switching

In the early 1990s, a few more methods, besides chaotic masking, were proposed for establishing secure communication, collectively known as 'chaotic regime switching' [145]. One such scheme is presented in Fig. 3. The transmitter

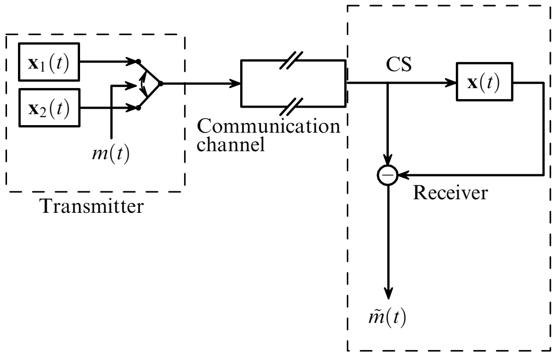

**Figure 3.** Schematic of a secure communication system based on chaotic regime switching.

[2] In what follows, confidentiality means the impossibility of a third party detecting information from a signal transferred through a communication channel.

contains two chaotic oscillators, $\mathbf{x}_1(t)$ and $\mathbf{x}_2(t)$, that may be either different or identical but have different parameters. Identical oscillators find wider application as assuring a higher degree of confidentiality; moreover, the signals they produce must have similar spectral and statistical characteristics. The useful digital signal $m(t)$ in the form of a sequence of binary bits 0/1 is used to switch over the signal being transmitted; in other words, the signal produced by the first chaotic oscillator encodes, for instance, the binary bit 0, while the signal from the second chaos oscillator encodes the binary bit 1. The resulting signal is transmitted through the communication channel toward the receiver. A few secure communication schemes based on chaotic regime switching are distinguished, depending on the number of oscillators resided on a side of the receiver. The scheme in Fig. 3 shows a receiving system comprising one chaotic oscillator $\mathbf{x}(t)$ identical to any transmitting one, for instance, to the first. The parameters of the oscillators must be selected in such a way as to produce signals leading to a complete chaotic synchronization regime only when a single binary bit is transferred (either a 0 or a 1). Similar to a chaotically masked procedure, the recovered signal $\tilde{m}(t)$ is obtained after the passage of the transmitted signal through the subtractor and the synchronous response of the chaotic oscillator in the receiver.

Other secure communication schemes utilizing chaotic regime switching are based on the same principle and differ from the described one only in the structure and operation of the receiving module. For example, the system covered in monograph [23] has a receiver with two chaotic oscillators identical to the transmitting ones and, therefore, two subtractors for the detection of the desired signal. In this case, the valid signal is diagnosed from the presence or absence of chaotic oscillations in the signals at the output of the receiver.

Such data transmission schemes are more stable to noise in the communication channel than chaotically masked systems; nevertheless, their robustness against noise is very limited. The critical drawback of such schemes is that switching results in an implementation of transient (sometimes rather lengthy) processes [152, 153] manifested as delayed locking of the receiving oscillator in synchronism. For this reason, such schemes operate rather slowly [23]. Moreover, their level of secrecy (confidentiality) is rather low [154].

### 3.3 Nonlinear mixing of an information signal with a chaotic one

Improvement of the chaotic masking technique was aimed at raising the level of secrecy and confidentiality during information transmission. As a consequence, a few methods have been proposed, presently known under the general name of 'nonlinear mixing of an information signal with a chaotic one'. Such systems are distinctive for the direct introduction of the information signal into the transmitting system and its participation in the formation of the output signal [23, 146].

Amongst the schemes in which a variety of operations are employed (summation/subtraction, multiplication/division, modulo-2 addition, voltage-to-current conversion, etc.), those using summation/subtraction operations are most widespread [125, 146]. In such schemes, the information signal is combined with the chaotic one and thereby contributes to the formation of the system's complicated behavior. The simplest and technically feasible method of realizing 'nonlinear mixing' is to place an additional chaotic oscillator at the transmitter end of the communication channel, the oscillator that is identical to the first transmitting oscillator and reciprocally coupled to it. A schematic of this method is presented in Fig. 4.

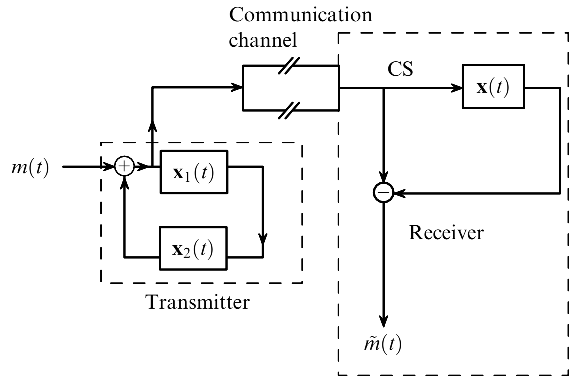

**Figure 4.** Schematic of a secure communication system using nonlinear mixing of an information signal with a chaotic one.

Briefly, the transmitting side contains two chaotic oscillators $\mathbf{x}_1(t)$ and $\mathbf{x}_2(t)$ identical in terms of control parameters. The information signal $m(t)$ is combined with the signal produced by one of the oscillators of the transmitter (or to both signals at a time). As the signal passes through the feedback loop (maintained by reciprocal coupling of transmitting oscillators), it undergoes nonlinear changes. The resulting signal formed by nonlinear mixing of the information signal with the chaotic one is further transmitted in the communication channel toward the receiver containing, as in the above schemes, a chaotic oscillator $\mathbf{x}(t)$ identical to the transmitting oscillators in terms of control parameters. The incoming signal synchronizes the receiving oscillator if a 0 binary bit is transferred, and does not affect a 1 binary bit transfer. The recovered signal $\tilde{m}(t)$ is detected after the signals from the transmitting and receiving oscillators pass the subtractor.

An important advantage of such schemes over chaotically masked systems is the possibility of varying the level of the introduced information message and thereby of controling communication quality (i.e., to vary the accuracy of deciphering the original message by its recipient). However, improved transmission quality of information leads to a loss of its confidentiality (a substantial fault [23]). Moreover, such schemes tend to show rather low robustness against noise contamination in the communication channel and a control parameter mismatch between the initially identical chaotic oscillators. The identity of three chaotic oscillators, two of which are located on different sides of the communication channel, is hard to achieve and may be regarded as one more disadvantage of the scheme.

Also, since the transmitting oscillator is essentially a nonautonomous device that does not guarantee formation of the chaotic signal alone when one or the other of the parameters of the system changes, the dependence of the transmitted signal on the information one may lead to a loss of confidentiality.

### 3.4 Modulation of the control parameters of a transmitting oscillator with an information signal

Schemes using modulation of the control parameters (or adaptive methods) constitute a natural step in the transition from discrete modulation of the control parameter of the

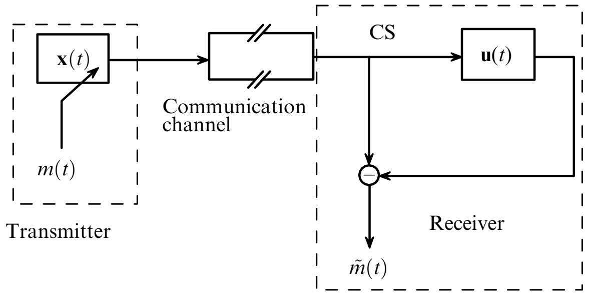

**Figure 5.** Schematic of a secure communication system using modulation of the control parameter of the transmitting oscillator with the information signal.

transmitting oscillator in chaotic regime switching (Section 3.2) to modulation with a continuous signal [147]. In this case, the information signal plays the role of the modulation signal. Preliminary determination of the permissible range of parameter variations and normalization of the modulating information signal are mandatory for the realization of such schemes. A peculiar case is the use of a binary digital signal as the information signal to modulate the control parameter of the transmitting oscillator. This secure communication scheme is shown in Fig. 5. Its operating principle is analogous to that described in Section 3.2 (chaotic regime switching). The valid digital signal $m(t)$ modulates one of the parameters of the transmitting oscillator $\mathbf{x}(t)$ in such a way that the complete chaotic synchronization regime may (or may not) establish itself between the transmitting $[\mathbf{x}(t)]$ and receiving $[\mathbf{u}(t)]$ oscillators, depending on the binary bit 0(1) being transferred. Then, the signals of the transmitting and receiving devices having passed through the subtractor, the recovered signal $\tilde{m}(t)$ is detected. In order to realize the complete synchronization regime, the control parameters of the receiving oscillator are chosen to be identical to those of the transmitting oscillator (more precisely, to a set of parameters of the transmitting oscillator, e.g., corresponding to binary bit 0).

The operating characteristics and merits and demerits of the schemes relying on modulation of control parameters are the same as in the case of chaotic regime switching. However, these schemes are somewhat easier to implement technically due to the presence of a single oscillator on the transmitting side of the communication channel.

## 4. The employment of other types of chaotic synchronization for secure information transmission

Main types of secure communication schemes based on complete chaotic synchronization were considered in Section 3. Other schemes using this principle are variants of the known ones differing only in the technical details of their realization. Section 3 presented a description of the simplest schemes providing a basis for the employment of chaotic synchronization in secure information transmission. As stated in Section 3, none of them is free of drawbacks. Further studies are aimed at developing new schemes devoid of these disadvantages; some of them ensure a higher degree of confidentiality, others show enhanced robustness against noise, still others do not require identity of oscillators, which simplifies their practical implementation. The most logical option in this case is to use a different type of synchronous behavior instead of complete chaotic synchronization. Some, even if not many such studies, are described in the literature. By way of example, it was proposed to apply phase synchronization to secure information transmission [155].

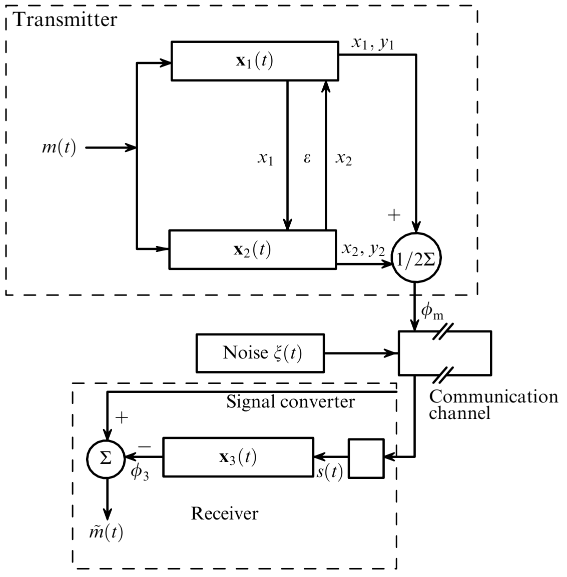

**Figure 6.** Schematic of a secure communication system based on chaotic phase synchronization.

This approach is illustrated by Fig. 6. The transmitting side of the communication channel has two identical reciprocally coupled oscillators with 1.5 degrees of freedom, each characterized by the state vectors $\mathbf{x}_{1,2}(t) = (x_{1,2}\,, y_{1,2}\,, z_{1,2})$. A dissipative coupling between the oscillators ensures phase synchronization at a sufficiently small coupling parameter $\varepsilon$. One of the control parameters of these oscillators (the same in either system) is modulated with valid digital signal $m(t)$. The instantaneous phase $\phi_{\mathrm{m}}(t)$ of signal $\mathbf{x}_{\mathrm{m}}(t) = (x_{\mathrm{m}}, y_{\mathrm{m}}, z_{\mathrm{m}})$ is employed as the transmitted signal. This signal represents the mean value of signals $\mathbf{x}_{1,2}(t)$ generated by these systems [the phase is introduced into consideration on plane $(x_{\mathrm{m}}, y_{\mathrm{m}})$, where $x_{\mathrm{m}} = (x_1 + x_2)/2$, and $y_{\mathrm{m}} = (y_1 + y_2)/2$]. Signal $\phi_{\mathrm{m}}(t)$ thus obtained and containing the desired information is transferred through the communication channel (where it is subjected to the effect of noises) toward the receiver containing chaotic oscillator $\mathbf{x}_3(t) = (x_3, y_3, z_3)$ identical to the transmitting oscillators, thus providing the occurrence of phase synchronization between them. The signal directly affecting the receiving chaotic oscillator is $s(t) = \eta(r_3 \cos\phi_{\mathrm{m}} - x_3)$, where $r_3 = (x_3 + y_3)^{1/2}$, and $\eta$ is the signal amplitude. The recovered signal $\tilde{m}(t)$ is obtained from the analysis of the behavior of phase difference $\Delta\phi = \phi_{\mathrm{m}} - \phi_3$ between the respective signals.

As follows from this description, the operating principle of phase synchronization-based secure communication schemes is essentially different from that of the schemes considered in Section 3. Nevertheless, this method has most of the drawbacks inherent in the schemes based on complete chaotic synchronization and is more difficult to realize (specifically, it requires experimental determination of the chaotic signal phase, generation of signal $s(t)$, and the presence of additional identical oscillators on opposite sides of the communication channel). Therefore, this scheme is not considered here in greater detail.

Some authors made attempts to employ generalized synchronization, besides phase one, for secure information transmission [98]. This approach opens up new research opportunities lacking in complete and phase synchronization-based schemes. First, generalized synchronization, unlike complete chaotic synchronization, occurs in quite different interacting dynamical systems [126], making possible simplification of practical implementations of secure communication methods based on this type of synchronous behavior. Second, the form of functional dependence between the states of interacting systems for generalized synchronization may be rather complicated, including fractal one [156]. This significantly limits the possibility for third party to obtain information about characteristics of the receiving oscillator from the time realization of the transmitted signal, i.e., it improves confidentiality. Third, the behavior of the generalized synchronization boundary on the plane of 'detuning frequency–communication intensity' parameters is anomalous and significantly different from the behavior of the boundaries of all known types of synchronous behavior. Specifically, the threshold for establishing the generalized synchronization regime at relatively low frequency detuning values in certain systems is roughly twice that in terms of the coupling parameter at a greater frequency detuning [157, 158]. This feature accounts for the emergence or decay of the synchronous regime in the case of very weak modulation of the control parameter, thus guaranteeing efficacious modulation of the control parameter for information transfer over communication channels. Finally, it will be shown in Section 5 that noise has practically no effect on the threshold for establishing the generalized synchronization regime. In other words, the synchronous regime arises in unidirectionally coupled dynamical systems at similar coupling strengths regardless of the presence or absence of noise (see also Refs [159, 160]); hence, the possibility of extremely noise-stable generalized synchronization-based schemes. Moreover, additional noise may be used for additional masking of the transmitted signal.

It should be noted, however, that the majority of the known secure communication methods based on the generalized synchronization regime do not use in full measure all its advantages. The most important of them are considered below in Sections 4.1 and 4.2.

### 4.1 Generalized synchronization-based secure communication method

Reference [109] is among a few, not numerous studies in which the generalized synchronization regime is used for secure information transmission. The essence of this method is illustrated in Fig. 7. The transmitter has two not necessarily identical chaotic oscillators, the driver $\mathbf{x}(t)$ and the responder $\mathbf{u}(t)$. A signal from the former is transmitted to the latter, while its intensity is modulated with the valid digital signal $m(t)$ in the following way: if a 0 binary bit is transferred, the generalized synchronization regime becomes established between the drive and response oscillators, but if a 1 binary bit is transmitted, the generalized synchronization regime between them is destroyed. The so-called auxiliary chaotic oscillator $\mathbf{v}(t)$ placed on the receiving side of the communication channel is identical to the drive oscillator in terms of control parameters. As a signal from the drive oscillator is transmitted through the communication channel to the auxiliary one, it gives rise to the generalized synchronization regime between them, with the intensity of the transmitted signal being the same as the intensity of a signal delivered to the response system during 0 binary bit transfer. The signal from the response oscillator passes to the receiver through another communication channel. Similar to secure communication schemes based on complete chaotic synchronization, two chaotic signals reach the receiver, one bearing the desired information, the other lacking it. Therefore, the valid digital signal $\tilde{m}(t)$ is easy to obtain by subtracting one incoming signal from the other.

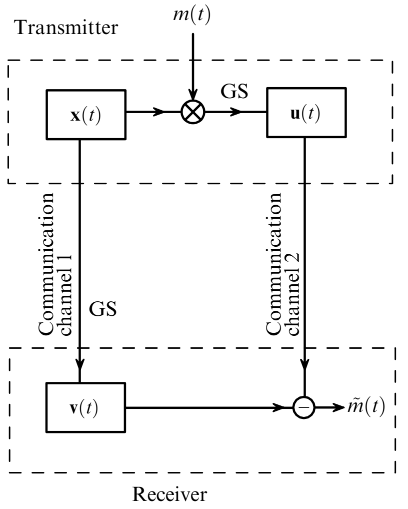

**Figure 7.** Schematic of a secure communication system using generalized chaotic synchronization as proposed in Ref. [109] (GS: generalized chaotic synchronization).

It can be seen that the auxiliary system method (see Section 2) is actively employed in the above secure communication scheme, which requires the presence of two chaotic oscillators identical in terms of control parameters. Similar to secure communication schemes based on complete chaotic synchronization, these oscillators are placed at opposite ends of the communication channel, which poses a serious technical problem: a small mismatch between control parameter values in these systems leads to the appearance of desynchronization noises[3], thus making such a scheme inoperative. Moreover, the necessity of having two communication channels is an important drawback, not only in terms of cost effectiveness but also because additional noise (sometimes of a quite different nature) may appear in the communication channel and corrupt the transmitted signal. In other words, such a scheme is rather sensitive to noise and difficult to put into effect.

Another concern is the confidentiality of information transfer. It is understandable that the employment of a different synchronous behavior and an additional communication channel may be advantageous in this context. However, the higher the quality of transmission, the lower the level of security as mentioned in Section 3.3 for the schemes using nonlinear mixing of an information signal with a chaotic one. In the present case, this problem is not as acute as it is in the systems based on complete chaotic synchronization regime (see Section 3).

[3] By desynchronization noise is meant the signal $\Delta\mathbf{x} = \mathbf{x}_2 - \mathbf{x}_1$, where $\mathbf{x}_{1,2}(t)$ are signals entering the subtractor (in the present case, signals from response and auxiliary chaotic oscillators plus noise in the communication channel). In a synchronous regime, one has $\Delta\mathbf{x} = 0$.

### 4.2 The use of several types of synchronous behavior for secure communication

The confidentiality of an information transfer can be enhanced using a few types of synchronous behavior simultaneously. By way of example, secure communication methods proposed in Refs [109, 161] make use of generalized and complete chaotic synchronization regimes at the same time.

The approach described in Ref. [109] (Fig. 8) is a modified version of a previously discussed scheme (see Section 4.1). The transmitting module operates on the same principle as that described in Section 4.1. Modification of the receiving system consists in using an additional chaotic oscillator $\mathbf{x}_2(t)$ identical to the drive oscillator $\mathbf{x}_1(t)$ as regards control parameters (hereinafter referred to as the second drive oscillator). A signal generated by the drive system is transmitted through the communication channel 1, whereupon the second drive oscillator moves into the complete synchronization regime. Confidentiality can be increased by feeding different signals to the response and second drive oscillators (e.g., the response system receives a signal representing the $x$-coordinate of the drive system, and the second drive oscillator admits a signal representing the $y$-coordinate).[4] On the receiving side of the communication channel, a signal from the second drive oscillator acts on the auxiliary oscillator and thereby establishes the generalized synchronization regime between them. A signal from the response oscillator is transmitted through the communication channel 2 toward the receiver. The signals reaching the drive and auxiliary oscillators being identical (as in the above case), the receiving side obtains two signals, one bearing useful information, the other lacking it. Therefore, the valid signal is readily detected after passage through the subtractor.

Clearly, such a scheme is more efficacious from the standpoint of maintaining information confidentiality, since it reduces the risk of interception of a communication by a third party. However, a number of other problems remain unresolved. The presence of two communication channels and identical oscillators in the transmitting and receiving systems (i.e., two pairs of identical oscillators), along with low robustness against noise in the communication channel that further decreases after destruction of complete chaotic synchronization, accounts for the impracticability of this and similar schemes for secure information transfer.

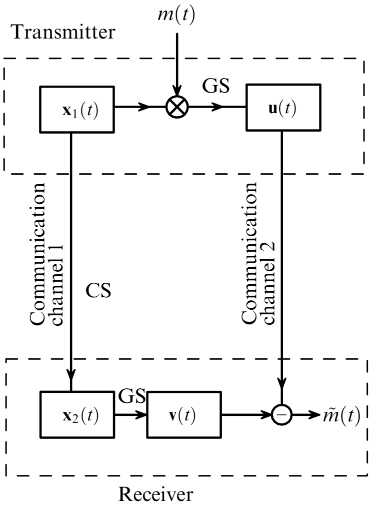

**Figure 8.** Schematic of a secure communication system based on generalized and complete chaotic synchronization, as proposed in [109].

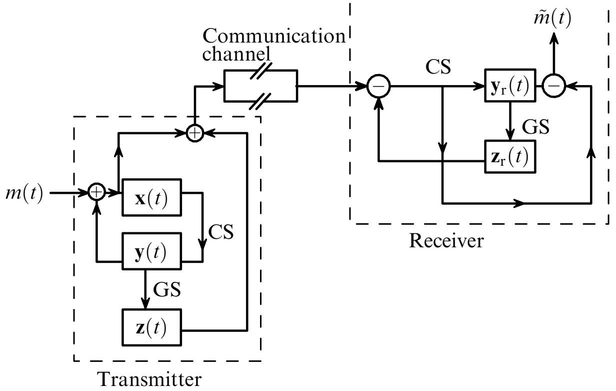

**Figure 9.** Schematic of a secure communication system using a compound chaotic signal.

The authors of Ref. [161] proposed an alternative approach to secure information transfer using two types of synchronous behavior — generalized and complete chaotic synchronization; this is, in fact, a modified secure communication scheme based on the nonlinear mixing of the information signal with the chaotic one (see Section 3.3).

This method is diagrammatically presented in Fig. 9. The transmitter contains two reciprocally coupled identical chaotic oscillators, $\mathbf{x}(t)$ and $\mathbf{y}(t)$ (hereafter, the first and the second), as in the scheme using the nonlinear mixing of the information signal with the chaotic one (see Section 3.3). The information signal $m(t)$ is combined with the signals from these oscillators and thereby undergoes nonlinear changes. There is one more oscillator $\mathbf{z}(t)$ on the transmitting side of the communication channel (referred to as the third one below), which is unidirectionally coupled to the second one but nonidentical to the first and second oscillators in terms of control parameters. The values of control parameters of transmitting oscillators must be chosen in such a way that the second and third oscillators are in the generalized chaotic synchronization regime, while the first and the second ones are in the complete synchronization regime. The third oscillator serves to enhance confidentiality; it forms a signal that in the simplest case is combined with the information-bearing signal. In this way, a compound signal is produced and an additional masking effect is achieved.

In Ref. [161], this original mode of data transmission was called "secure communication using a compound signal from generalized synchronizable chaotic systems". The compound signal is transmitted over the communication channel to the receiver containing two oscillators: the fourth $\mathbf{y}_{\rm r}(t)$ identical to the first and the second in terms of control parameters, and the fifth $\mathbf{z}_{\rm r}(t)$ identical to the third one with respect to the same parameters. Oscillators 4 and 5 are in the generalized synchronization regime. Then, according to the auxiliary system method, oscillators 3 and 5 will undergo identical oscillations due to the identity of systems 4 and 2. Signals from the communication channel and oscillator 5 come to the subtractor. Signals reaching oscillator 4 and subtractor 2 contain no additional components. The signal acting on

[4] It may correspond to voltage signals taken at different points of the oscillator circuit.

oscillator 4 synchronizes it when the 0 binary bit is transmitted, and fails to cause synchronization when bit 1 is transmitted. The restored signal $\tilde{m}(t)$ at the output constitutes a sequence of fragments showing synchronous (binary bit 0) and nonsynchronous (binary bit 1) behavior.

It follows from the above that such a scheme ensures a rather high level of confidentiality: in the majority of cases it does not allow a third party to diagnose a message transmitted through the communication channel from the compound signal even in the absence of noise. As in the case of nonlinear mixing of a signal, however, the quality of information transfer (hence, the possibility of recovering high-quality information) strongly depends on the desired level of confidentiality, i.e., the higher it is, the lower the quality is. Formation of the compound signal permits somewhat weakening this dependence. This gives a slight advantage of this scheme over the others, which, however, does not compensate for a number of its drawbacks. The involvement of five oscillators, two and three of which must be identical, poses a practically insolvable technical problem, especially if the oscillators are to be located on different sides of the communication channel. The introduction of even a small parameter mismatch between these oscillators would immediately make the scheme inoperative. Furthermore, noises in the communication channel would inevitably cause distortion of the transmitted signal and would therefore destroy complete synchronization between the second and the fourth oscillators and generalized synchronization between the fourth and the fifth oscillators. Signals on opposite sides of the channel would lose identity and detection of the message in the receiver would become impossible.

Thus, the partial correction of certain imperfections eventually leads to the aggravation of others. Practical realization of the schemes under consideration characterized by high enough level of confidentiality is an extremely difficult task due to their low robustness against noise and the mismatch between control parameters. For this reason, an 'extensive' approach to the improvement of secure communication methods (e.g., the use of several types of synchronous behavior) appears nonoptimal.

## 5. Extremely noise-stable secure communication method

Analysis of secure communication schemes in Sections 3 and 4 indicates that they share some specific features, characteristic differences, merits, and demerits, despite the use of different types of synchronous behavior. First and foremost, these are:

- a high degree of identity of chaotic oscillators on different sides of the communication channel;
- a low robustness against noise in the communication channel;
- a low level of confidentiality, i.e., the possibility in certain cases of reconstructing parameters of the transmitting oscillator from the transmitted signal, especially in complete chaotic synchronization-based schemes, and, in the end, of a third party decoding the information signal.

In this section, we shall consider a secure communication method essentially free of these disadvantages [162, 163]. In addition, it is characterized by high robustness against noise and, as a consequence, a high degree of confidentiality. The method leans upon generalized synchronization but, unlike that described in Section 4, takes into account all the peculiarities of the generalized synchronization regime; hence, its fundamental advantages over the known analogs.

The description of the method itself is preceded by a brief discussion of the causes behind structural stability of the generalized synchronization regime to noise.

### 5.1 Noise-stable generalized synchronization regime

As is well known, generalized synchronization regime is evidenced in systems with dissipative and nondissipative coupling [126, 164]. For the former, the equations describing the dynamics of interacting systems in the presence of noise have the form

$$\begin{aligned} \dot{\mathbf{x}}(t) &= \mathbf{G}\big(\mathbf{x}(t),\, \mathbf{g}_{\mathrm{d}}\big)\,, \\ \dot{\mathbf{u}}(t) &= \mathbf{H}\big(\mathbf{u}(t),\, \mathbf{g}_{\mathrm{r}}\big) + \varepsilon A\big(\mathbf{x}(t) - \mathbf{u}(t) + D\xi(t)\big)\,, \end{aligned} \tag{3}$$

where $\mathbf{x}(t)$ and $\mathbf{u}(t)$ are the state vectors of the drive and response systems, respectively, $\xi(t)$ is the noise signal, $\mathbf{G}$ and $\mathbf{H}$ are the vector fields of the interacting systems, $\mathbf{g}_{\mathrm{d}}$ and $\mathbf{g}_{\mathrm{r}}$ are the vectors of the control parameters, $A = \{\delta_{ij}\}$ is the coupling matrix, $\delta_{ii} = 0$ or $\delta_{ii} = 1$, $\delta_{ij} = 0$ $(i \neq j)$, $\varepsilon$ is the coupling parameter, and $D$ is the noise intensity.

The mechanisms of the origination of a generalized synchronization regime are elucidated using the modified system method proposed for the first time in our studies [164, 165]. In this method, the response system $\mathbf{u}(t)$ is regarded as a certain modified system:

$$\dot{\mathbf{u}}_{\mathrm{m}}(t) = \mathbf{H}'\big(\mathbf{u}_{\mathrm{m}}(t),\, \mathbf{g}_{\mathrm{r}}, \varepsilon\big)\,, \tag{4}$$

subjected to the external action $\varepsilon\big(A\mathbf{x}(t)+D\xi(t)\big)$:

$$\dot{\mathbf{u}}_{\mathrm{m}}(t) = \mathbf{H}'\big(\mathbf{u}_{\mathrm{m}}(t),\, \mathbf{g}_{\mathrm{r}}, \varepsilon\big) + \varepsilon\big(A\mathbf{x}(t) + D\xi(t)\big)\,, \tag{5}$$

where $\mathbf{H}'\big(\mathbf{u}(t)\big) = \mathbf{H}\big(\mathbf{u}(t)\big) - \varepsilon A\mathbf{u}(t)$. The term $-\varepsilon A\mathbf{u}(t)$ introduces additional dissipation into the modified system (4).

The generalized synchronization regime evolving in system (3) may be regarded as a product of two simultaneous interrelated processes, viz. enhanced dissipation in the modified system (4) and the growing amplitude of an external (chaotic and noise) signal. The two processes are related by parameter $\varepsilon$ and cannot be realized separately in the response system (3). However, enhancement of dissipation in the modified system (4) simplifies its behavior and causes it to move from chaotic to periodic oscillations (or to the stationary state). Conversely, the external action tends to complicate the behavior of the modified system and impose its own dynamics. Evidently, the origination of a generalized synchronization regime is feasible only when the natural chaotic dynamics in the response system are suppressed as a result of dissipation.

Thus, the stability of a generalized synchronization regime is first of all determined by the properties of the modified system itself. Therefore, the emergence threshold for a generalized synchronization regime should be virtually independent of noise intensity $D\xi(t)$ affecting unidirectionally coupled chaotic systems. If the noise does not alter characteristics of the modified system (4), it should not substantially influence the emergence threshold of a generalized synchronization regime.

As mentioned in Section 2, on-line diagnostics of the generalized synchronization regime is possible both by the auxiliary system method and by calculating conditional Lyapunov exponents. Clearly, response and auxiliary systems may be regarded as two identical systems with similar initial conditions. Taking a derivative of the difference between their states $\mathbf{\Delta}(t) = \mathbf{v}(t) - \mathbf{u}(t)$ with $(D > 0)$ and without $(D = 0)$ noise leads (due to the identity of deterministic and stochastic signals acting on these systems) to one and the same equation

$$\dot{\mathbf{\Delta}}(t) = \big(\mathbf{JH}(\mathbf{u}(t)) - \varepsilon A\big)\,\mathbf{\Delta}(t) = \mathbf{JH}'\big(\mathbf{u}(t)\big)\,\mathbf{\Delta}(t)\,, \tag{6}$$

where $\mathbf{J}$ is the Jacobian matrix. Because equation (6) can be regarded as a variational equation in the computation of conditional Lyapunov exponents, it may be concluded that senior conditional Lyapunov exponents determining the emergence threshold for a generalized synchronization regime should exhibit identical behavior in both the presence and absence of noise. Therefore, the threshold must be unrelated to noise intensity and the type of the synchronous behavior has to show high robustness against the noise.

The validity of theoretical interpretation is confirmed by numerical simulation [160, 166] and the results of physical experiment [159]. A number of studies have demonstrated that the generalized synchronization regime is structurally noise-stable both in systems with a small number of degrees of freedom [160] and in spatially distributed media [159]. Experimental verification of this observation was achieved in a radiotechnical study using low-frequency chaos oscillators [160].

### 5.2 Description of the method

Let us now move to describing the extremely noise-stable secure communication method. A block diagram of its realization is presented in Fig. 10.

In Ref. [162], this method is described as follows. The information signal $m(t)$ is encoded using the binary number system. One or a few control parameters of the transmitting oscillator $\mathbf{x}(t)$ are modulated with the binary signal, so that the characteristics of the transmitted signal change only insignificantly. The signal thus obtained is transmitted through the communication channel, where it is distorted under the effect of noise. The receiver at the opposite end of the communication channel is composed of two identical oscillators, $\mathbf{u}(t)$ and $\mathbf{v}(t)$, capable of operating in the regime of generalized synchronization with the transmitting oscillator. The operating principle of the receiver is based on the on-line diagnostics of a generalized synchronization regime by the auxiliary system method (see Section 2). The signal from the communication channel comes to the receiving oscillators, the output signals pass through the subtractor, and the restored valid signal $\tilde{m}(t)$ becomes available for detection. [5]

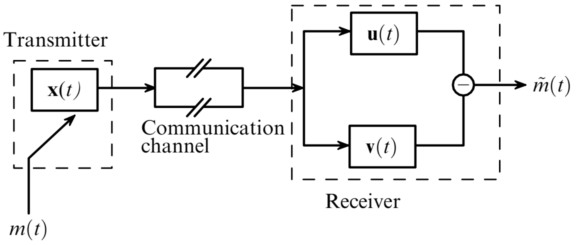

**Figure 10.** Schematic of an extremely noise-stable secure communication system based on generalized chaotic synchronization.

Modulation of the control parameters of the transmitting oscillators can be achieved, so as to ensure the emergence (absence) of a generalized synchronization regime between transmitting and receiving oscillators depending on the transmitted 0 (1) binary bit. For example, if the generalized synchronization regime occurs in the case of bit 0 transmission, both receiving oscillators undergo identical oscillations; after passage through the subtractor, chaotic oscillations are absent (i.e., the 0 binary bit is observed). Conversely, transmission of binary bit 1 is not associated with emergence of a generalized synchronization regime, whereas oscillations of the receiving oscillators are nonidentical; passage through the subtractor results in a nonzero amplitude of chaotic oscillations (i.e., the 1 binary bit).

An important advantage of the secure communication method under consideration is the possibility of having nonidentical oscillators on either side of the communication channel. Two identical oscillators are located on the receiving side, which facilitates their adjustment, eases identity requirements, and thereby simplifies practical realization of the method.

Furthermore, signals entering oscillators of the receiver are always identical even in the presence of noise in the communication channel. Therefore (see Section 5.1), given dissipative coupling between transmitting and receiving oscillators, the noise does not have an appreciable influence on the emergence threshold for a generalized synchronization regime. This peculiarity suggests the possibility of developing noise-stable methods of secure communication based on the generalized synchronization regime.

## 6. Comparison of known secure communication methods

This section is devoted to a comparative analysis of the operating capacity of chaotic synchronization-based secure communication methods described in this review. To verify their efficiency in the presence of noise in the communication channel, we shall employ numerical simulation and evaluate certain quantitative characteristics of the operating capacity of the schemes of interest. In all cases, unidirectionally coupled Rössler systems serve as transmitting and receiving oscillators with similar control parameter values, [6] while simple binary bit sequences will be used as information signals. The choice of such models of radio electronic oscillators is dictated by the following considerations: (1) the Rössler systems are fairly well studied, including but not limited to chaotic synchronization regimes (see Refs [97, 129, 140, 157, 165, 167, 168]); (2) the unidirectionally coupled Rössler systems allow all types of synchronous behavior, providing a basis for all the secure communication schemes considered in this review [98, 131, 138, 140, 157, 164, 167–169]; (3) the location of generalized synchronization bound-

[5] It is worthwhile to mention some analogy between this technique and the method based on modulation of control parameters, described in Section 3.4. In both cases, control parameters of the transmitting oscillators are modulated with a binary signal, but in the former a generalized synchronization regime is employed, in contrast to a complete synchronization regime in the latter. It helps to obviate a number of drawbacks mentioned in Section 3.4.

[6] The detailed description of these systems and the values of control parameters can be found in Sections 6.1, 6.2.

ary on the plane of 'detuning frequency–communication intensity' parameters satisfies the requirements expounded in Section 4 (see also Ref. [158]), and (4) a radio electronic oscillator whose dynamics are described by Rössler equations is conceivable [170]. Such a choice will enable us to properly compare the schemes considered with each other and, moreover, to check the efficiency of their operation for real devices [170].

### 6.1 Numerical realization of the extremely noise-stable secure communication method

We shall start from a numerical realization of the most efficacious extremely noise-stable secure communication method that does not require identical oscillators at the ends of the communication channel (see Section 5.2, Fig. 2). In this case, the transmitting oscillator is described by the following system of differential equations:

$$\begin{aligned}\dot{x}_1 &= -\omega_x x_2 - x_3\,,\\ \dot{x}_2 &= \omega_x x_1 + a x_2\,,\\ \dot{x}_3 &= p + x_3(x_1 - c)\,,\end{aligned} \tag{7}$$

where $\mathbf{x}(t) = (x_1, x_2, x_3)$ is the state vector of the transmitting oscillator, the control parameters $a = 0.15$, $p = 0.2$, and $c = 10$, and $\omega_x$ is the control parameter characterizing the eigenfrequency of system oscillations.

Parameter $\omega_x$ is modulated with the information digital signal in the following way. If a 1 binary bit is transmitted during a given time interval, then $\omega_x = 0.95$ throughout this interval. For bit 0 transfer, $\omega_x = 1$. Such values of the parameter $\omega_x$ are chosen just for the sake of demonstration as dictated by the location of the generalized synchronization boundary studied in detail in Ref. [158]. As a matter of fact, parameter $\omega_x$ can assume practically any value (e.g., results similar to those discussed below were obtained for $\omega_x = 0.91$ and $\omega_x \in [0.9, 0.91]$ for bit 1 and 0 transmissions, respectively. The sole necessary condition is the alternation of regions with asynchronous dynamics and a generalized synchronization regime.

The receiver contains two identical chaotic oscillators, each described by the following system of equations:

$$\begin{aligned}\dot{u}_1 &= -\omega_u u_2 - u_3 + \varepsilon\big(s(t) - u_1\big)\,,\\ \dot{u}_2 &= \omega_u u_1 + a u_2\,,\\ \dot{u}_3 &= p + u_3(u_1 - c)\,.\end{aligned} \tag{8}$$

Here, $\mathbf{u}(t) = (u_1, u_2, u_3)$ is the state vector of the first receiving oscillator. Let $\mathbf{v}(t) = (v_1, v_2, v_3)$, also satisfying equation (8), be the state vector of the second receiving oscillator (see Fig. 10). Control parameters $a$, $p$, and $c$ are chosen to be identical with the corresponding parameters of the transmitting oscillator. Control parameter $\omega_u$ characterizing the eigenfrequency of the receiving oscillators is chosen to equal $\omega_u = 0.95$ throughout the period of signal transmission.

A signal generated by the transmitting oscillator propagates through the communication channel. In the model of interest (7), (8), this process is realized via coupling between the transmitting and receiving oscillators, i.e., by the introduction of component $\varepsilon(s(t) - u_1)$ into the first equation of system (8). Here, $s(t) = x_1 + D\xi$ is the signal in the communication channel. The term $D\xi$ simulates intrachannel noises; $\xi$ is the stochastic Gaussian process characterized by the probability distribution

$$p(\xi) = \frac{1}{\sqrt{2\pi}\sigma}\exp\left[-\frac{(\xi - \xi_0)^2}{2\sigma^2}\right], \tag{9}$$

where $\xi_0 = 0$ and $\sigma = 1$ are the average and variance.[7] Parameter $D$ determines the intensity of the added noise.

Coupling strength between transmitting and receiving oscillators is given by parameter $\varepsilon$, chosen to equal 0.14. Then, in the absence of noise and fluctuations in the communication channel ($D = 0$), the generalized synchronization regime in systems (7) and (8) occurs at $\omega_x = 1$, but disappears at $\omega_x = 0.95$ (see Ref. [158] for details).

The subtractor performs operation $(u_1 - v_1)^2$. In accordance with the auxiliary system method, after a signal passes through the subtractor there must be chaotic oscillations for $\omega_x = 0.95$ and no oscillations whatever for $\omega_x = 1$. The restored signal will be a sequence of fragments showing different types of behavior.

The simple sequence of binary bits 0/1, chosen as the original message, is displayed in Fig. 11a. Stochastic equation (8) is integrated by the Euler method with a time discretization interval $h = 0.0001$ [171].

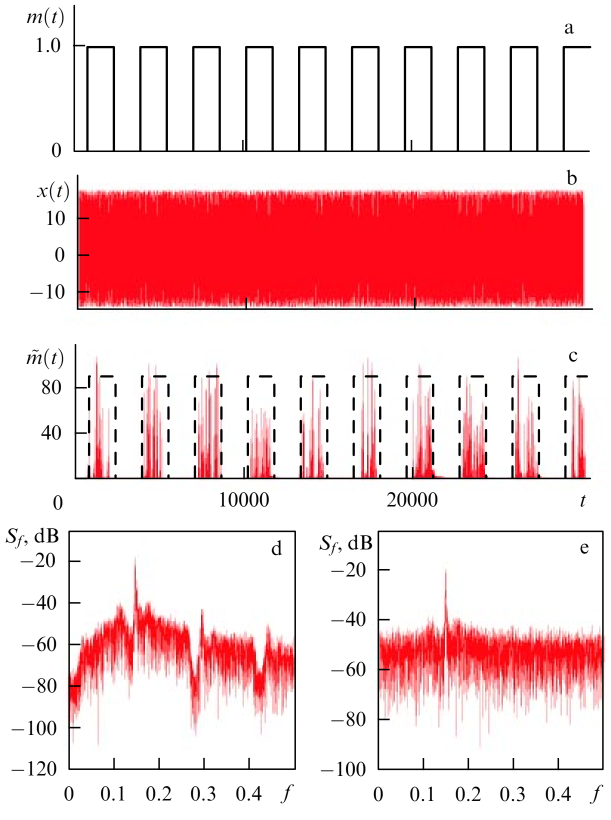

**Figure 11.** Numerical realization of a secure communication method based on generalized chaotic synchronization in the absence of noise and fluctuations in the communication channel ($D = 0$): (a) information signal $m(t)$ represented by a simple sequence of binary bits 0/1; (b) signal $x(t)$ produced by the transmitting oscillator for subsequent transfer through the communication channel, and (c) restored signal $\tilde{m}(t)$ and detected information signal (dashed line). Signal power spectra in the channel in the absence (d) and presence (e) of noise with intensity $D = 10$.

[7] Notice that the distribution patterns of the stochastic quantity $\xi$ are of little importance, and similar results were obtained for other (e.g., uniform) types of probability density $p(\xi)$.

Let us start from an idealized situation with the absence of noise in the communication channel (noise amplitude $D = 0$). Evidently, such a situation does not occur in practice in noisy engineering devices. However, it is the use of idealized schemes with 'noiseless' communication channels that enabled practically all known secure information transfer schemes to be proposed and tested, although the influence of noise on their performance was, as a rule, neglected: hence, the importance of idealized situations to verify operating capacity of a given scheme and compare it with the previously used secure communication methods.

The operating capacity of a noiseless scheme is illustrated in Fig. 11b, c. Signal $x(t)$, generated by the transmitting system for transmission over the communication channel, is shown in Fig. 11b. Characteristics of this signal remain practically unrelated to the transmitted 0/1 binary bit ($\omega_x$ changes), as is well apparent from the absence of traces of amplitude and frequency modulation in signal $x(t)$. Owing to relatively small frequency detuning, the power spectrum of this signal contains a single clearly visible component (Fig. 11d), which precludes decoding the message by a third party. Figure 11c depicts signal $\tilde{m}(t)$ restored in the receiver; by passing it through a low-pass filter and correctly choosing threshold values, it is easy to detect the original message.[8]

Let us consider now the influence of noise inevitably present in communication channels of real devices on the efficiency of the generalized synchronization-based scheme for secure information transfer. Evidently, any noise causes dramatic distortion of the signal being transferred, thereby worsening the quality of data transmission and sometimes making it altogether impossible (as will be shown in Section 6.2, this assertion holds true for all other schemes described in this review). However, the noise has practically no effect on the emergence threshold for the generalized synchronization regime in dissipatively coupled chaotic systems (see Section 5.1), i.e., the synchronous regime evolves in such systems with and without noise at roughly similar values of the coupling parameter $\varepsilon$. At the same time, stability analysis of the system considered reveals situations where noise having a sufficiently high amplitude not only leaves the generalized synchronization regime undestroyed but, on the contrary, causes it to arise at lower coupling strengths than are necessary for generalized synchronization to appear in the absence of noise. It may have a negative effect on the quality of data transmission, i.e., lead to the possibility of detecting the 0 binary bit alone.[9] However, the noise must have a very large amplitude in order to 'strengthen' generalized synchronization. As appears from the results of investigations, for system (7), (8) with the above control parameter values such a situation takes place at the noise amplitude $D > 400$.

The operating capacity of the secure data transmission system under consideration in the presence of rather strong noise in the communication channel ($D = 10$) is illustrated in Fig. 12. As in Fig. 11, this figure shows information signal $m(t)$ (Fig. 12a), signal $s(t)$ (Fig. 12b) transmitted through the communication channel (i.e., the signal generated in the transmitting module (Fig. 11b) plus intrachannel noise), and the restored signal $\tilde{m}(t)$ before (solid line) and after (dashed line) passage through a low-pass filter and the choice of threshold values. The addition of noise with a sufficiently high amplitude makes the signal transmitted through the communication channel practically indiscernible from the stochastic one in terms of both temporal realization and close-to-Gaussian amplitude distribution (cf. Figs 12d and 12e showing similar distributions in the absence and presence of noise). The power spectrum of such a signal (Fig. 11e) exhibits, as in the absence of noise, a single clearly visible component, while the addition of noise only leads to an increase in the noise pedestal present in the signal. In this case, detection of the desired information by a third party is virtually impossible. At the same time, the quality of information recovered in the receiver remains as high as in the absence of noise in the communication channel (cf. Figs 11c and 12c). A similar situation takes place at any noise intensity $D$ in a range from 0 to 400. It confirms once again the high stability of generalized synchronization-based secure communication systems to intrachannel noises and underlines the contribution of noise to the improvement of communication confidentiality without the loss of information transmission quality.

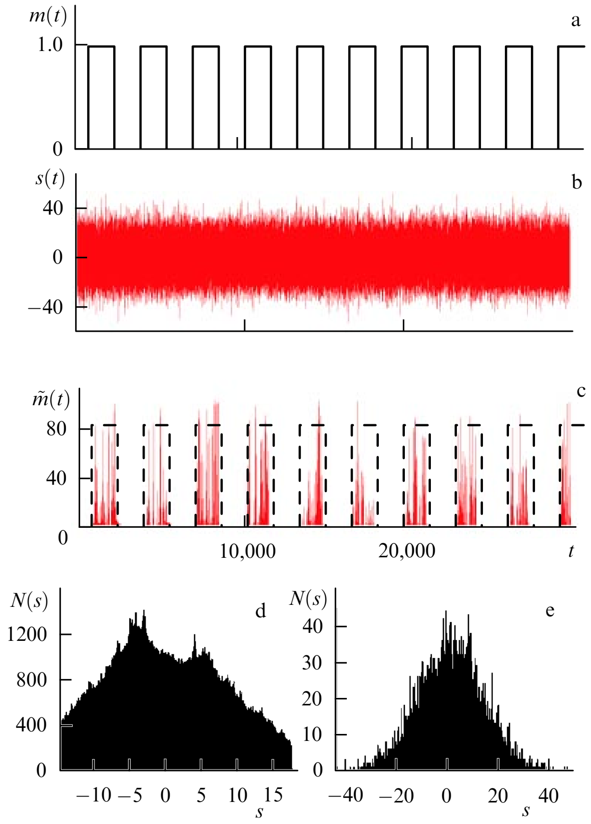

**Figure 12.** Numerical realization of a secure communication method based on generalized chaotic synchronization in the presence of strong noise in the communication channel ($D = 10$): (a) information signal $m(t)$ represented by a simple sequence of binary bits 0/1; (b) signal $s(t)$ transmitted through the communication channel; (c) restored signal $\tilde{m}(t)$; detected information signal is marked by the dashed line. Distribution of signal amplitudes in the communication channel in the absence (d) and presence (e) of noise with intensity $D = 10$ in the channel.

### 6.2 Numerical realization of other chaotic synchronization-based methods of secure communication

Let us move to the numerical simulation of other chaotic synchronization-based methods of secure information trans-

[8] The initial information signal shown in Fig. 11a exactly coincides with the detected signal in Fig. 11c (dashed line), which suggests a high quality of data transmission.

[9] Whenever other schemes become inoperative, only a 1 binary bit is detected.

fer, described in this review. To begin with, numerical realization of schemes using chaotic masking (Section 3.1), chaotic regime switching (Section 3.2), modulation of control parameters (Section 3.4), and two more systems proposed in Ref. [109] and considered in Sections 4.1 and 4.2 does not lead to a significant change of equations for transmitting and receiving oscillators. Therefore, we assume (unless otherwise stated) that all of them are described by the sets of differential equations (7), (8) with respective control parameters $a = 0.15$, $p = 0.2$, $c = 10$, and $\omega_u = 0.95$. The values of other control parameters strongly depend on the type of synchronous behavior used in a given method and the peculiarities of its realization; it necessitates their choice for each individual system separately. The same refers to the character of the signal in the communication channel. However, we shall use in all cases a digital signal represented by a simple sequence of binary bits 0/1 as the information signal and assume that intrachannel noise obeys distribution (9).

To implement the chaotically masked secure communication method (see Section 3.1, Fig. 2), the communication channel must have two identical oscillators on its different sides. Therefore, $\omega_x = 0.95$ is chosen for the entire period of signal transmission. Chaotic masking is accomplished by a direct mixing of the information signal with chaotic one in order to have the intrachannel signal in the form $s(t) = x_1 + m(t) + D\xi$. Moreover, coupling strength between the systems needs to be increased if the complete chaotic synchronization regime is to be realized; therefore, we choose $\varepsilon = 0.25$.

The scheme using chaotic regime switching as the base (Section 3.2, Fig. 3) has a transmitting module with two oscillators, one of which is in complete chaotic synchronization with the receiving oscillator (i.e., is its exact replica, $\omega_x = 0.95$) and encodes the binary bit 0. The second transmitting oscillator is not identical to the receiving one and is not synchronized with it (therefore, we choose $\omega_x = 1$ in this case), encoding the binary bit 1. The intrachannel signal has then the form $s(t) = x_1 + D\xi$, and coupling strength between the systems is chosen (by analogy with chaotically masked schemes) to be $\varepsilon = 0.25$.

For the method leaning upon modulation of control parameters (Section 3.4, Fig. 5), it is appropriate to choose the same parameter values as in the case of chaotic regime switching, because numerical realization of these two modes of data transmission in a secure manner are virtually identical (provided the latter regime uses two identical transmitting oscillators with slightly mismatched parameters). Hence, the choice of $s(t) = x_1 + D\xi$, $\varepsilon = 0.25$, and

$$\omega_x = \begin{cases} 0.95, & m(t) = 0, \\ 1.00, & m(t) = 1. \end{cases}$$

The scheme based on the generalized chaotic synchronization regime [109] (see also Section 4.1, Fig. 7) implies the presence of an additional chaotic oscillator identical to the receiving one on the transmitting side of the communication channel. We shall designate oscillators of the transmitting module as drive and response ones, by analogy with Ref. [109]; the oscillator on the receiving side, identical to the response oscillator, will be referred to as auxiliary. Then, the drive oscillator is described by the system of equations (7) with the aforementioned parameter values and $\omega_x = 1$ (to ensure nonidentity with other oscillators); the response and auxiliary oscillators are described by the system of equations (8), but the signals $s(t)$ taking effect on them will be different: $s(t) = n(t)x_1$, where

$$n(t) = \begin{cases} 0.9, & m(t) = 1, \\ 1.0, & m(t) = 0 \end{cases}$$

if they affect the transmitting oscillator, and $s(t) = x_1 + D\xi$ if they are fed via the communication channel to the receiving oscillator. The coupling parameter is chosen to be $\varepsilon = 0.14$ (as in the method described in Section 6.1) to make possible generalized synchronization between nonidentical oscillators.

The scheme starting from generalized and complete chaotic synchronization (see Ref. [109] and Section 4.2, Fig. 8) includes an additional oscillator on the transmitting side of the communication channel; it is identical to the first transmitting one in terms of control parameters and is unidirectionally coupled to it (hereafter — the second drive oscillator). This oscillator is described by the system of equations (7) containing an additional term, namely

$$\begin{aligned} \dot{y}_1 &= -\omega_x y_2 - y_3 + \varepsilon_2\big(g(t) - y_1\big)\,, \\ \dot{y}_2 &= \omega_x y_1 + a y_2\,, \\ \dot{y}_3 &= p + y_3(y_1 - c)\,, \end{aligned} \tag{10}$$

where $\mathbf{y}(t) = (y_1, y_2, y_3)$ is the state vector of this oscillator, $\varepsilon_2 = 0.2$ is the parameter characterizing coupling strength between 'drive' oscillators, and $g(t) = x_1 + D\xi$ is the signal transmitted through the first communication channel. In this case, signal $s(t)$ is also somewhat changed, and the auxiliary oscillator is affected by signal $s(t) = y_1$.

Simulation of both schemes proposed in Ref. [109] requires taking into account the presence of the second communication channel, meaning that the signal transmitted from the response oscillator to the receiver is also contaminated with noise. Therefore, the subtractor admits not only deterministic signals generated by the response and auxiliary oscillators, but also a stochastic signal from the second communication channel. The restored signal then has the form $\tilde{m}(t) = (u_1 + D\xi - v_1)^2$, disregarding the difference between noises in the two communication channels (taking it into account significantly impairs the possibility of detecting the desired signal).

In numerical simulation of the schemes based on the mixing of the information signal with the chaotic one (see Section 3.3, Fig. 4), the transmitting module is described by the following systems of differential equations:

$$\begin{aligned} \dot{x}_1 &= -\omega_x x_2 - x_3 + \varepsilon\big(y_1 + m(t) - x_1\big)\,, \\ \dot{x}_2 &= \omega_x x_1 + a x_2\,, \\ \dot{x}_3 &= p + x_3(x_1 - c)\,, \\ \dot{y}_1 &= -\omega_x y_2 - y_3 + \varepsilon\big(x_1 + m(t) - y_1\big)\,, \\ \dot{y}_2 &= \omega_x y_1 + a y_2\,, \\ \dot{y}_3 &= p + y_3(y_1 - c). \end{aligned} \tag{11}$$

In other words, it consists of two identical reciprocally coupled chaotic oscillators. Here, $\mathbf{x}(t) = (x_1, x_2, x_3)$ and $\mathbf{y}(t) = (y_1, y_2, y_3)$ are the state vectors of the first and second transmitting oscillators, respectively, $m(t)$ is the information signal, $\omega_x = 1.00$, and $\varepsilon = 0.25$. The receiving oscillator is described by system (8), with $\omega_u = 1$. The signal in the communication channel constitutes the simple sum of the signal generated by one of the chaotic transmitting systems and the intrachannel noises, i.e., $s(t) = x_1 + D\xi$.

The method of secure information transfer proposed in Ref. [161] (see also Section 4.2, Fig. 9) only slightly complicates the scheme of nonlinear mixing of the information signal with the chaotic one because it implies the use of two more identical oscillators on different sides of the communication channel. Therefore, the equations and parameters of the three oscillators utilized in both variants remain unaltered. The additional oscillator on the transmitting side of the communication channel is described by the following system of equations:

$$\begin{aligned} \dot{z}_1 &= -\omega_z z_2 - z_3 + \varepsilon(y_1 - z_1)\,, \\ \dot{z}_2 &= \omega_z z_1 + a z_2\,, \\ \dot{z}_3 &= p + z_3(z_1 - c)\,, \end{aligned} \qquad (12)$$

where $\mathbf{z}(t) = (z_1, z_2, z_3)$ is the state vector of this oscillator, and $\omega_z = 0.95$. The analogous oscillator on the receiving side, characterized by the state vector $\mathbf{v}(t) = (v_1, v_2, v_3)$, also satisfies system (12) up to the replacements $\mathbf{z}(t) \to \mathbf{v}(t)$, $\mathbf{y}(t) \to \mathbf{u}(t)$, where $\mathbf{u}(t) = (u_1, u_2, u_3)$ is the state vector of the receiving oscillator described by the set of equations (8), but in this case one has $s(t) = y_1 + z_1 - v_1 + D\xi$. Signal $-v_1$ is not transmitted over the communication channel; it is added after passage through it before arriving at the receiving oscillator.

Numerical realization of the secure information transmission technique based on chaotic phase synchronization (see Section 4, Fig. 6) was achieved in Ref. [155] using Rössler systems with close values of the control parameters as examples. In this case, oscillators of the transmitting and receiving modules are described by the following sets of equations:

$$\begin{aligned} \dot{x}_{1,2} &= -(\omega_x + \Delta\omega)\, y_{1,2} - z_{1,2} + \varepsilon(x_{2,1} - x_{1,2})\,, \\ \dot{y}_{1,2} &= (\omega_x + \Delta\omega)\, x_{1,2} + a y_{1,2}\,, \\ \dot{z}_{1,2} &= p + z_{1,2}(x_{1,2} - c)\,, \\ \dot{x}_3 &= -\omega_u y_3 - z_3 + \eta(r_3 \cos\phi_{\mathrm{m}} - x_3)\,, \\ \dot{y}_3 &= \omega_u x_3 + a y_3\,, \\ \dot{z}_3 &= p + z_3(x_3 - c)\,, \end{aligned} \qquad (13)$$

where $\mathbf{x}_{1,2} = (x_{1,2}, y_{1,2}, z_{1,2})$, $\mathbf{x}_3 = (x_3, y_3, z_3)$ are the state vectors of oscillators entering these modules, respectively, $\omega_x = \omega_u = 1$, $\varepsilon = 5 \times 10^{-3}$, and $\eta = 5.3$ are the coupling parameters, $\Delta\omega = \pm 0.01$ is the $\omega_x$-parameter mismatch modulated with the valid digital signal (the plus sign corresponds to the transmission of a 1 binary bit, the minus sign to a 0 binary bit), and $r_3 = (x_3^2 + y_3^2)^{1/2}$ is the amplitude of the signal generated by the receiving system. Notice that most data needed for the comparison of this scheme with a number of analogs described in the present review can be found in paper [155]. Therefore, evaluation of the operating capacity of this scheme is to a large extent based on these findings.

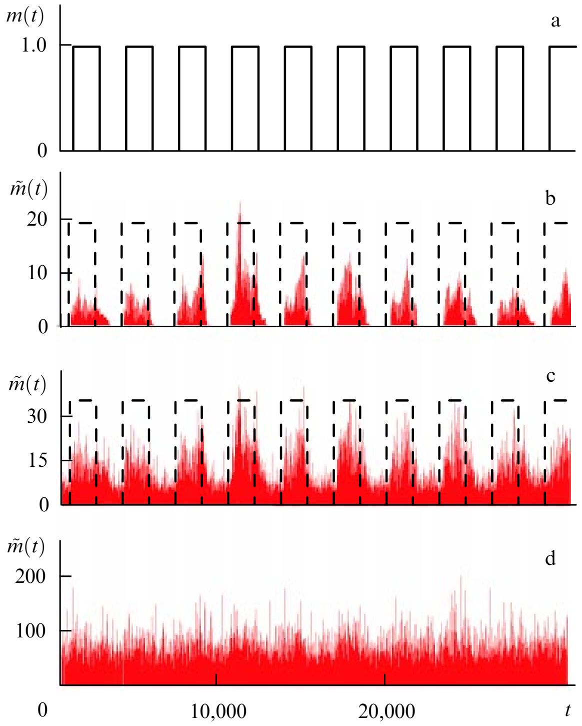

**Figure 13.** The influence of intrachannel noise on the efficiency of a secure communication system based on generalized chaotic synchronization proposed in Ref. [109]. Information signal $m(t)$ represented by a simple sequence of binary bits 0/1 (a), and restored signal $\tilde{m}(t)$ at different noise amplitudes: $D = 0$ — absence of intrachannel noise and fluctuations (b), $D = 1.5$ — low-intensity noise (c), and $D = 3$ — higher-intensity noise (d). The information signal (dashed line) can be detected in cases (b) and (c) but not in (d).

Numerical realization of all the rest of the secure communication techniques with the above control parameters confirms their limited robustness against noise.[10] Moreover, noise influences them very similarly in qualitative terms, despite the use of different types of synchronous behavior and quite different operating principles.

The most demonstrable example of the noise effect on the operating capacity of secure communication using generalized chaotic synchronization proposed in paper [109] is presented in Fig. 13. It displays the information signal $m(t)$ represented by a simple sequence of binary bits (Fig. 13a), and restored signals $\tilde{m}(t)$ (solid lines) at different noise amplitudes (Fig. 13b–d). This method performs rather efficiently in the absence of noise in the communication channel (Fig. 13b). In this case, the information signal is easy to detect from the absence or presence of chaotic oscillations in the signal $\tilde{m}(t)$. The signal thus restored is shown by the dashed line. It is readily seen that the quality of information transfer is rather high even if erroneous diagnosing of binary bit 1 remains possible in scattered instances due to transient processes.

The appearance of noise in a communication channel gives rise to the creation of desynchronization noise. If the noise intensity is rather small, the possibility of decoding the message $m(t)$ by the restored signal $\tilde{m}(t)$ will still be left over. As evident from Fig. 13c corresponding to the case of

[10] Integration of stochastic differential equations simulating transmitting and receiving oscillators is in all cases performed (as in Section 6.1) by the Euler method with a time discretization interval $h = 0.0001$.

$D = 1.5$, in spite of the presence of desynchronization noise in all the signal $\tilde{m}(t)$, the fragments of the latter related to a 0 binary bit are characterized by lower amplitudes. Therefore, the information signal may be detected in proper selection of the threshold value; the restored signal in Fig. 13c is shown as a dashed line.

A further increase in noise amplitude leads to 'equalization' of oscillation amplitudes in the regions corresponding to binary bits 0 and 1 (see, for instance, Fig. 13d showing signal $\tilde{m}(t)$ at $D = 3$). Clearly, there is no possibility of decoding the valid massage in this case.

A qualitatively analogous situation takes place with all secure communication methods considered in Sections 3 and 4. Thus, it can be concluded, based on the available studies, that noise in a vast majority of cases has a negative effect on secure information transmission. However, more characteristics need to be evaluated for quantitative comparison of these schemes.

### 6.3 Quantitative characteristics of systems' performance

The major quantitative characteristics of the operating capacity of secure communication systems include:

(1) A critical $\mathrm{SNR_c}$ value (energy-per-bit to spectral-noise-power-density ratio) [172, 173] at which a secure communication system becomes inoperative, i.e., restoration of the initial valid digital signal $m(t)$ from the output signal $\tilde{m}(t)$ becomes impossible. The energy-per-bit to spectral-noise-power-density ratio introduced in the consideration for digital communication systems is an analog of the signal-to-noise ratio in analog communication:

$$\mathrm{SNR} = 10 \lg \frac{E_\mathrm{b}}{N_0} \; [\mathrm{dB}] \,, \tag{14}$$

where $E_\mathrm{b}$ is the signal energy per bit of transmitted information, and $N_0$ is the spectral noise power density. The energy per bit is described as follows:

$$E_\mathrm{b} = P_\mathrm{sign} T \,, \tag{15}$$

where $\mathrm{P_{sign}}$ is the transmitted signal power in the absence of noise, and $T$ is the bit transmission time; the spectral noise power is defined as

$$N_0 = \frac{P_\mathrm{noise}}{\Delta f} \,, \tag{16}$$

where $P_\mathrm{noise}$ is the noise power in the communication channel, and $\Delta f$ is the bandwidth of the communication channel. Because noise is inevitably present in communication channels of real devices, estimation of the operating capacity of noise-contaminated secure communication systems is a challenging problem.

The power of both deterministic and stochastic signals is evaluated by their temporal realization. It was assumed for the purpose of numerical computation that the bandwidth $\Delta f = f_2 - f_1 = 0.2$, where $f_1 = 0.05$, $f_2 = 0.25$ are the bandwidth boundaries of the communication channel, when Rössler oscillators are employed.

Apart from the above characteristic, the dependence of the bit error rate (BER) on the energy-per-bit to spectral-noise-power-density ratio is frequently used to estimate the degree of stability of secure communication schemes to external noise in digital communication systems [174]. BER is the number of errors referred to the number of transmitted bits and characterizes the quality of information transfer. Suppose that a system adequately transmits a 0 binary bit with probability $P_{00}$, and a 1 binary bit with probability $P_{11}$. Then, the probability of erroneous diagnosing of bit 1 during transmission of bit 0 is $P_{01} = 1 - P_{00}$, and the probability of erroneous detection of bit 0 during transmission of bit 1 is $P_{10} = 1 - P_{11}$. If the symbols appear in the sequence being transmitted with probabilities $P_0$ and $P_1$, respectively, the error probability per bit is given by

$$\mathrm{BER} = 2(P_{01} P_0 + P_{10} P_1) \,, \tag{17}$$

and probabilities $P_{01}$ and $P_{10}$ depend on the type and parameters of the communication system.

(2) Maximum $\mathrm{PM_c}$ (control parameter mismatch) value (PM,%) between oscillators assumed to be originally identical. As shown in Sections 3 and 4, in the majority of instances such oscillators must be located on opposite sides of the communication channel. The influence of control parameter mismatch on the efficiency of information transmission systems is a topical problem, bearing in mind the technical difficulties encountered in their realization.

(3) Maximum $\mathrm{ND_c}$ (nonlinear distortion) level in the communication channel, at which the system is operative:

$$\mathrm{ND} = 10 \lg \frac{P_x}{P_y} \; [\mathrm{dB}] \,. \tag{18}$$

Here, $P_x$ is the power of signal $x(t)$ at the output of the transmitting oscillator, and $P_y$ is the power of signal $y(t)$ at the input of the receiving oscillator. Nonlinear distortions in the form of cubic nonlinearity $y = x(1 - \alpha x^2)$, where $\alpha$ is a small parameter [23], are traditionally included in numerical calculations; therefore, it is assumed below that a signal undergoes distortions of such a type when it passes through communication channels of all schemes and devices.

Let us estimate the aforementioned characteristics of all the systems described in the review in order to quantitatively compare different secure communication methods. To recall, the authors of monograph [23] introduced a different characteristic of operating capacity of data transmission systems based on the degree of signal similarity defined as

$$\eta = \frac{\Delta P}{P} \,, \tag{19}$$

where $\Delta P$ is the desynchronization noise power, and $P$ is the noise power at the oscillator input. However, this characteristic makes sense only for systems leaned upon complete chaotic synchronization and is not considered here in order to achieve generality and facilitate comparison of different methods.

Estimated quantitative efficiency characteristics of the systems of interest are presented in Table 1 below.

It can be seen that scheme 9 described in Section 5.2 becomes inoperative at the energy-per-bit to spectral-noise-power-density ratio $\mathrm{SNR_c} = -10.01$ dB. For all other schemes, $\mathrm{SNR_c}$ has a positive value. In other words, most schemes become inoperative in the presence of noise of a certain level in the communication channel, even if their power is lower than that of the transmitted signal. Clearly, $\mathrm{SNR_c}$ values vary from one scheme to another. Schemes based on chaotic regime switching and modulation of control parameters (Nos 2 and 4 with $\mathrm{SNR_c} = 30.76$ dB) appear to be the

**Table 1.** Critical values of energy-per-bit to spectral-noise-power-density ratio (SNR$_c$), control parameter mismatch (PM$_c$) between initially identical oscillators, and nonlinear distortion level (NDc) in the communication channel.

| No. | Scheme | SNR$_c$, dB | PM$_c$, % | ND$_c$, dB | Section* | Reference |
|---|---|---|---|---|---|---|
| 1 | Chaotic masking | 56.8 | 0.30 | 1.03 | 3.1 | [25] |
| 2 | Chaotic regime switching | 30.76 | 2.00 | 23.3 | 3.2 | [145] |
| 3 | Nonlinear mixing | 64.99 | 0.30 | 0.26 | 3.3 | [146] |
| 4 | Modulation of control parameters | 30.76 | 2.00 | 23.3 | 3.4 | [147] |
| 5 | Phase synchronization-based scheme | 32.40 | 0.80 | 10.7 | 4 | [155] |
| 6 | Generalized synchronization-based scheme | 39.52 | 1.00 | 7.75 | 4.1 | [109] |
| 7 | Generalized and complete synchronization-based scheme | 39.24 | 0.50 | 4.83 | 4.2 | [109] |
| 8 | Scheme with a ‘compound signal’ | 61.47 | 0.20 | 2.63 | 4.2 | [161] |
| 9 | Extremely noise-stable scheme | −10.01 | 2.00 | 27.2 | 5.2 | [162] |

* Section of the present review.

most efficient among schemes 1 – 8. However, positive SNR$_c$ is indicative of limited robustness against noise and the destructive role of noise during information transfer.

Scheme 9 (see Section 5.2) is highly stable to noise present in the communication channel. Noise in the channel causes distortion of the signal being transmitted and thereby preclude message decoding by a third party. In this case, noise plays a positive role, enhancing confidentiality of information transfer; in all other schemes, it produces a destructive effect.

This inference is also confirmed by the dependence of the bit error rate on spectral noise power density in various secure communication schemes. Such dependences are illustrated in Fig. 14. In calculation of BER, the threshold value allowing restoration of the initial sequence of binary bits by signal $\tilde{m}(t)$ was assumed to be fixed regardless of noise intensity; it was varied in calculating the tabulated characteristics. As follows from Fig. 14, BER rapidly tended toward unity in the majority of secure communication schemes (1 – 8), but was close to zero in the extremely noise-stable scheme 9 regardless of noise intensity in the system, in excellent agreement with the above results.

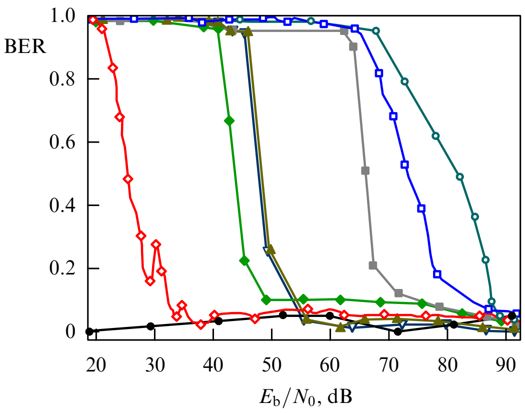

**Figure 14.** Plots of bit error rate (BER) versus energy-per-bit to spectral-noise-power-density ratio ($E_b/N_0$) for different secure communication schemes: ○ — chaotic masking, ◆ — chaotic regime switching (modulation of control parameters), ■ — nonlinear mixing, ◇ — phase synchronization-based scheme (the curve is partly borrowed from Ref. [155]), ▲ — generalized synchronization-based scheme, △ — generalized and complete synchronization-based scheme, □ — compound signal-based scheme, and ● — extremely noise-stable scheme.

Let us estimate the effect of control parameter mismatch on the performance of secure communication systems described in this review. To this end, a mismatch is introduced into parameter $\omega_u$ of one of the two initially identical systems (if there are two pairs of identical systems then each pair is mismatched in terms of parameter $\omega$). Then, parameter $\omega$ of one system is replaced by the parameter $\omega(1 \pm \eta)$, where $\eta$ is the mismatch of $\omega$ (PM). For definiteness, a plus sign will be chosen in all cases (similar results are obtained using a minus sign).

Such estimation gives evidence that the system based on generalized synchronization regime (see Section 5) remains operative until $\omega_u$-parameter mismatch between oscillators of the receiving module exceeds 2%. Certainly, it is not a large mismatch, and the scheme being considered has competitors as regards this characteristic, for example, secure communication systems based on chaotic regime switching and modulation of control parameters (schemes 2 and 4 in Table 1). However, scheme 9 has an indisputable advantage in this respect, too. The initially identical chaotic oscillators in schemes 2 and 4 (and in all the rest, besides 9) must be located on different sides of the communication channel to enable realization of complete synchronization between them. Scheme 9 contains identical oscillators only on the receiving side of the communication channel, which considerably simplifies their adjustment, if needed.

The scheme described in Section 5 also surpasses all known analogs in terms of robustness against nonlinear distortions in the communication channel. Evidently, the greater the effect of nonlinear distortions on a signal, the higher their maximally permissible level at which the secure communication system remains operative. Table 1 shows that the maximum level of nonlinear distortions for scheme 9 is ND$_c$ = 27.2 dB. Schemes based on chaotic regime switching and modulation of control parameters (schemes 2 and 4) are closest to scheme 9 in terms of this characteristic; however, resistance of the latter system to nonlinear distortions is slightly higher. Moreover, schemes 2 and 4 possess limited robustness against noise, whereas it is practically unlimited in scheme 9.

Clearly, changes in control parameters and equations for oscillators can lead to changes in quantitative values of the characteristics being analyzed, e.g., in all cases the transmitting and receiving modules may contain Chua's oscillators [175, 176], ring chaotic oscillators with delay [151, 177 – 179], phase-locked chaotic oscillators [180 – 183], or chaos oscillators with 2.5 degrees of freedom [184], etc. A similar effect may have a change in the distribution pattern of random variable $\xi$. At the same time, the absolute and relative values of these characteristics are always of the same order (see, e.g., Ref. [78]). Moreover, these results agree well with experimental findings concerning data transmission in the radio frequency band and optical range, as will be shown in Section 7. By way of example, the theoretically deduced high sensitivity of the operating capacity of complete and generalized synchronization-based systems to parameter mismatch between oscillators located on different sides of the communication channel is consistent with experimental data obtained under the guidance of A S Dmitriev at the Institute of Radioengineering and Electronics, Russian Academy of Sciences (IRE). This issue will be considered at greater length in Section 7.1. Thus far, suffice it to mention that the permissible mismatch between oscillators on different sides of the communication channel does not usually exceed 0.5–1% [23]. An increase in mismatch of even a single parameter by 3–4% in a scheme based on chaotic synchronous response leads to complete destruction of synchronization and the loss of operating capacity. This experiment utilized chaos oscillators as proposed by Chua. The synchronous regime was destroyed under the on–off intermittency scenario [185 – 187] characterized by the loss of synchronization at some instants of time [185, 188]. It should be noted that the use of ring chaos oscillators usually permits avoiding intermittent behavior [23].

## 7. Experimental realization of information transmission schemes based on chaotic synchronization

Thus, the fundamentals and various concrete schemes of information transfer using chaotic synchronization were considered in Sections 2–6. Detailed theoretical and numerical analysis of diverse various methods of information transfer based on this phenomenon revealed major merits and demerits of different systems and substantiated the employment of novel communication techniques taking advantage of generalized chaotic synchronization and being free of many drawbacks inherent in currently available schemes. This approach, based on numerical simulation and comparison of different schemes, provides many new opportunities. On the one hand, it made possible analysis of numerous schemes on a common basis and revealed in a uniform fashion advantages and disadvantages of individual methods (a goal unattainable in experimental studies for the difficulty of maintaining uniform conditions and building breadboard models of very distinctive schemes). On the other hand, numerical simulation and analysis are becoming increasingly more popular methods for designing and adjustment of modern telecommunication systems that allow for the application of computer-assisted technologies in the early period of work. There are many software packages for this purpose (MultiSim [11], Micro-Cap [12], Microwave Office [13]) used to simulate the schemes of interest at the stage of engineering design and to create fully operative breadboard models based on numerical calculations alone. In other words, numerical simulation provides a powerful tool for analysis and assessment of applications of the chaos theory to information transmission. Good examples of applying these technologies in scientific research were given, for example, in the monograph by A S Dmitriev and A I Panas [23]. Nevertheless, the necessity of pursuing experimental studies remain even more important than ever before. Investigations with the use of experimental models help to confirm theoretical predictions and substantiate underlying mathematical models and assumptions. In other words, an adequate combination of theoretical and experimental research followed by a detailed comparison of the data obtained is needed to come to a conclusion as regards practical applicability of one idea or another.

For this reason, we shall focus below on some important experimental studies of information transmission schemes using chaotic synchronization. The number of such studies is much smaller than that of numerical simulation research due, first of all, to the difficulty of practical implementation of relevant communication systems. A major concern is the development of efficacious oscillators of chaotic signals for such systems. The main requirements imposed on these oscillators are apparent from what was said in the previous sections, viz. the possibility of chaotic synchronization, the availability of developing identical and readily replicable oscillators, and their handleability necessary to feed an information signal into a chaotic one, etc. The best results have thus far been obtained in the radio frequency band and visible range, as opposed to the microwave range. It is therefore appropriate to consider examples of experimental realization of information transmission schemes and possibilities of synchronizing chaotic oscillations separately for electronic and optical systems.

### 7.1 Experimental realization of information transmission schemes in the radio frequency and microwave ranges

Most experimental studies on different methods of information transfer using chaotic synchronization have been conducted based on radiotechnical systems. Attempts were undertaken to realize some of the above schemes making use of complete chaotic synchronization. Systematic work on the realization and technical optimization of data transmission schemes with the employment of chaotic signals as information carriers was carried out by such methods as chaotic masking (and its modifications underlain by the synchronous response phenomenon [94]), chaotic regime switching, and the nonlinear mixing of an information signal with a chaotic one. Historically, chaotic masking was one of the earliest secure communication methods depending on the application of chaos synchronization; this accounts for the large number of experimental studies using this approach.

Paper [189] demonstrated the possibility of transferring messages by the chaotic masking and chaotic regime switching methods built around a Lorenzian low-frequency (LF) oscillator operating in the 0–10 kHz range. Figure 15 illustrates the working characteristics of this system, viz. test information signal $m(t)$ in the form of a bit sequence to modulate parameters of the transmitting oscillators, and square of the restored signal, $\tilde{m}^2(t)$. Signal state $m = 0$ corresponded to complete synchronization of the receiving system, and state $m = 1$ to asynchronous dynamics. The system clearly demonstrates the possibility of transmitting a

[11] www.ni.com/multisim

[12] www.spectrum-soft.com/index.shtm

[13] web.awrcorp.com/Russian

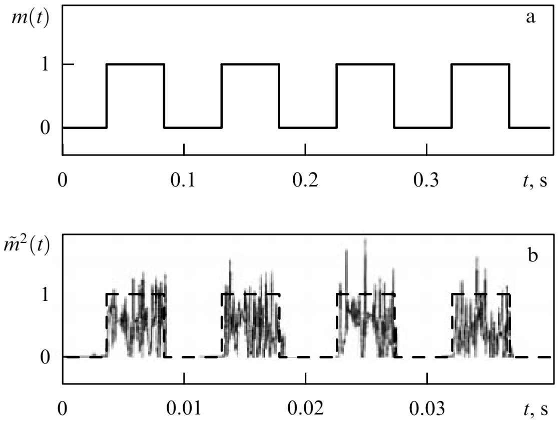

**Figure 15.** Experimental realization of an information transmission scheme based on chaotic regime switching: (a) information signal $m(t)$ represented by a simple sequence of binary bits 0/1, and (b) signal $\tilde{m}^2(t)$ restored in the receiving module (solid line). The dashed line shows the detected information signal. (Taken from Ref. [189].)

digital signal. The same electronic oscillators were used in Ref. [189] to realize a chaotically masked communication system for transmitting analog signals (speech messages). The transmitted and restored sound message: "He has the bluest eyes" is exemplified in Fig. 16a, b. This scheme proved operative only at a sufficiently high information signal/masking chaotic signal ratio (20–30 dB), which makes the transmitted signal commensurate with the noise level in the communication channel (Fig. 16c). Study [189] did not include experiments for the analysis of the robustness of these schemes against intrachannel noises and the nonidentity of oscillators. Special experiments designed to elucidate conditions necessary for complete chaotic synchronization-based information transfer schemes to operate were conducted for the first time in Ref. [148]. They revealed strict requirements for the signal/noise ratio, the identity of modules at both ends of the communication channel, etc. in chaotic masking, chaotic regime switching, and nonlinear mixing schemes, in excellent agreement with our theoretical findings.

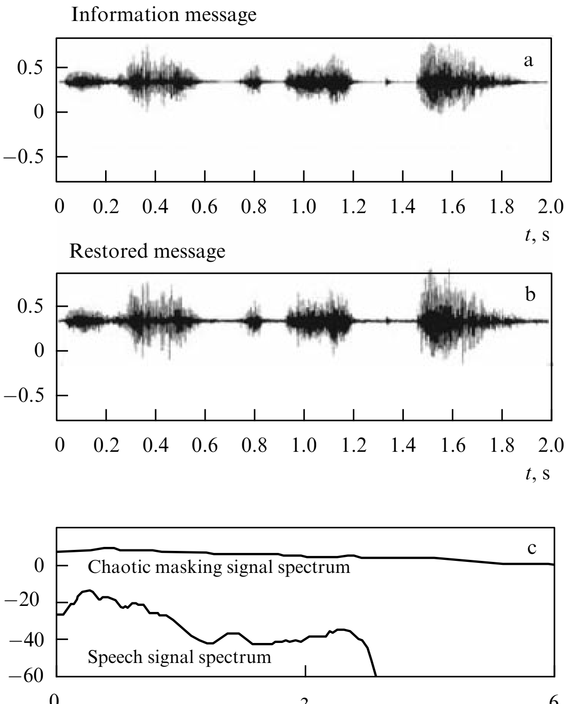

**Figure 16.** Results of experiments on analog information transfer by the chaotic masking method: speech message transmitted (a) and detected at the receiver output (b), and relationship between power spectra of information and chaotic masking signals (c). (Taken from Ref. [189].)

Detailed investigations of information transmission based on chaotic synchronization techniques, carried out by A S Dmitriev's group (IRE), were summarized in monograph [23]. These experiments included information transmission using chaos in the radio frequency band based on the nonlinear information mixing scheme in standard amplitude-modulated communication systems [146, 190]. The main concern regarding this scheme was signal distortion associated with chaotic LF signal transfer into the radio frequency band and back. The 27-MHz frequency was chosen as the working carrier frequency. During this procedure, the signals were subjected to additional manipulations (absent in the aforementioned LF experiments), viz. amplification, modulation, filtration, demodulation, etc., each causing new distortions that interfered with the detection of an exact replica of the transmitted chaotic signal in the receiver necessary to ensure complete chaotic synchronization. Of primary importance in such experiments is achieving the desired accuracy of direct and reverse transformations of the signal and taking into account noises and filtration in the communication channel. It was shown that total distortions along the signal transformation chain in the transmitting and receiving modules should not exceed 1–2% if the high-quality transfer of information is to be achieved; it imposes very strict limitations in terms of the practical implementation of the system. At the same time, experiments reported in Ref. [23] demonstrated the fundamental possibility of wired and wireless transmission of information in the radio frequency band using a nonlinear mixing scheme. They simultaneously exposed the difficulties and constraints inherent in this method.

By way of example, it was shown that the degree of correspondence between parameters of functionally analogous elements in the transmitting and receiving modules should not be less than 0.5%. However, even fulfillment of this condition did not guarantee the desired quality of complete chaotic synchronization due to the unsuccessful choice of chaos oscillators for transmitting and receiving modules in the Chua scheme [176, 191, 192]. This scheme produced no stable response but displayed on–off intermittency effects that markedly worsened the quality of communication reception. A very serious limitation on the system's performance was signal distortions in the communication channel, which manifested themselves as nonuniformities of amplitude–frequency characteristic of the channel (in fact, in filtration of the transmitted signal) and nonlinear distortions. Special experiments demonstrated that the efficiency of the scheme was determined by the relationship between cut-off frequency $\omega_c$ of the high-pass filter used to simulate distortions in the communication channel and upper boundary frequency $\Omega$ of the signal power spectrum at the output of the transmitting module. For $\omega_c \gg \Omega$, filtration had no effect on information transmission quality, but the commensurability of these quantities, $\omega_c \sim \Omega$, worsened the quality of signal detection [193].

Increasing nonlinear distortions also led to the rapid loss of the system's operating capacity. In particular, the signal-to-noise ratio at the output of the receiving module was 35–40 dB, when the coefficient of nonlinear distortions did not exceed 1% of the signal amplitude, and decreased to 10 dB when this coefficient was 10%. The experimental scheme of wireless information transmission had similar dynamics when the influence of additive normally distributed noise in the communication channel increased; namely, the signal-to-noise ratio at the output of the receiving module grew with the rise in noise power much faster than the same ratio in the communication channel, i.e., at the input of the receiver. This situation is due to the loss of quality during separation of the combined information signal from the chaotic one by establishing complete chaotic synchronization regime in the receiver. Here too, it was important to choose a more efficacious source of the chaotic signal in the transmitting and receiving modules.

A S Dmitriev and co-workers undertook an analysis of an important problem of choosing optimal electronic chaos oscillators for information transmission. As mentioned in Section 6.3, they arrived at the conclusion that the circular organization of such systems is especially efficacious due to their higher stability and absence of the breakdown of complete synchronization for parameter mismatch between the drive and response oscillators (on–off intermittency) [178]. The authors showed that the resistance of circular systems to parameter mismatch and external noises is roughly 2–3 times that of classical radiotechnical sources of chaos in the Chua scheme [23, 178, 194, 195]. Other important advantages of ring-type chaos oscillators are their precision defined by the authors of Refs [23, 196] as the reproducibility of similar chaotic regimes in different samples or after replacement of selected elements in a given oscillator, low sensitivity to changing ambient conditions (e.g., temperature), and a stable response to synchronization without its breakdown at certain instants of time. An alternative to the choice of chaos oscillators for communication systems is the employment of digital signal processors for the realization of information transfer systems with the nonlinear mixing of a signal [197].

These studies provided a basis for the creation of experimental breadboard models of communication systems operating in low-frequency and radio frequency bands that were used to demonstrate the fundamental possibility of transmitting information based on the nonlinear mixing of the information signal with the chaotic one [23]. A major concern was the contradictory requirement of high quality and confidentiality of information transmission because improvement in quality impaired the security and vice versa.

It should be emphasized that the function of the above chaotic communication systems operating in the low-frequency and radio frequency bands is mainly confined to validation of various technical decisions and the choice of optimal chaos oscillators or information transmission schemes. Evidently, secure information transmission methods based on synchronization of chaotic oscillations may be utilized for practical purposes in passing to the microwave range extensively employed in modern telecommunication systems. However, publications on chaos synchronization and methods using it for information transmission in the microwave range are practically absent in the literature, probably due to the difficulty of designing and conducting relevant experiments. Also, maintenance diagnostics of chaotic synchronization regimes in microwave chaos oscillators requires expensive digital measuring equipment and special analytical methods. To the best of our knowledge, the only studies in this area were reported in Refs [198, 199].

Larsen et al. [198] reported the first (and apparently thus far the sole) attempt to design a prototype system for information transmission employing chaos oscillators built around a powerful microwave amplifier (broadband traveling wave tube, TWT) applicable to long-distance information transmission, including satellite systems. A source of chaotic signals was a ring oscillator with time-delayed feedback based on the 2–4 GHz powerful TWT created at Wisconsin State University [200]. Microwave chaos oscillators built around a TWT with time-delayed feedback, which constituted the earliest sources of chaotic signals, were for the first time proposed by V Ya Kislov and co-workers at IRE [201 – 203]. They were later thoroughly investigated in Refs [200, 204 – 206]. Up to now, such oscillators remain the simplest powerful and reliable sources of chaotic signals in the microwave range. No wonder one of them was chosen for a prototype telecommunication system. The simplest chaotic masking technique (see Section 3.1) utilized for information transfer in Ref. [198] demonstrated the principal possibility of exploiting a scheme containing powerful vacuum microwave devices for chaotic synchronization-based information transmission. The design of the experiment was practically that described in Section 3.1 (see Fig. 2). The theoretical rationale for such a scheme with a TWT amplifier-based oscillator was provided earlier in Ref. [207]. The experimental setup is presented in Fig. 17 [198]. The information signal was mixed with a chaotic one in the time-delayed feedback loop enclosing the TWT amplifier. The chaotic microwave signal with the combined analog message was emitted from a horn antenna (Fig. 17) and forwarded to the receiver containing an almost exact replica of the transmitting oscillator. Preliminary studies demonstrated the possibility of secure information transmission in such a scheme based on complete chaotic synchronization. Unfortunately, the results of further experiments were not presented in Ref. [198].

At the same time, alternative methods for information transmission in the microwave range using other types of chaotic synchronization remain to be developed. Of primary importance in this context is the realization of generalized chaotic synchronization regimes in the microwave range for devices to be used as drive and response chaos oscillators in

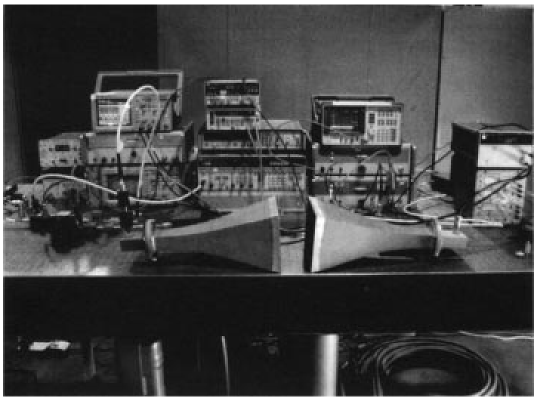

**Figure 17.** Experimental setup for secure information transfer by the chaotic masking method in the microwave range (2–4 GHz), which is based on a TWT with time-delayed feedback. (Taken from Ref. [198].)

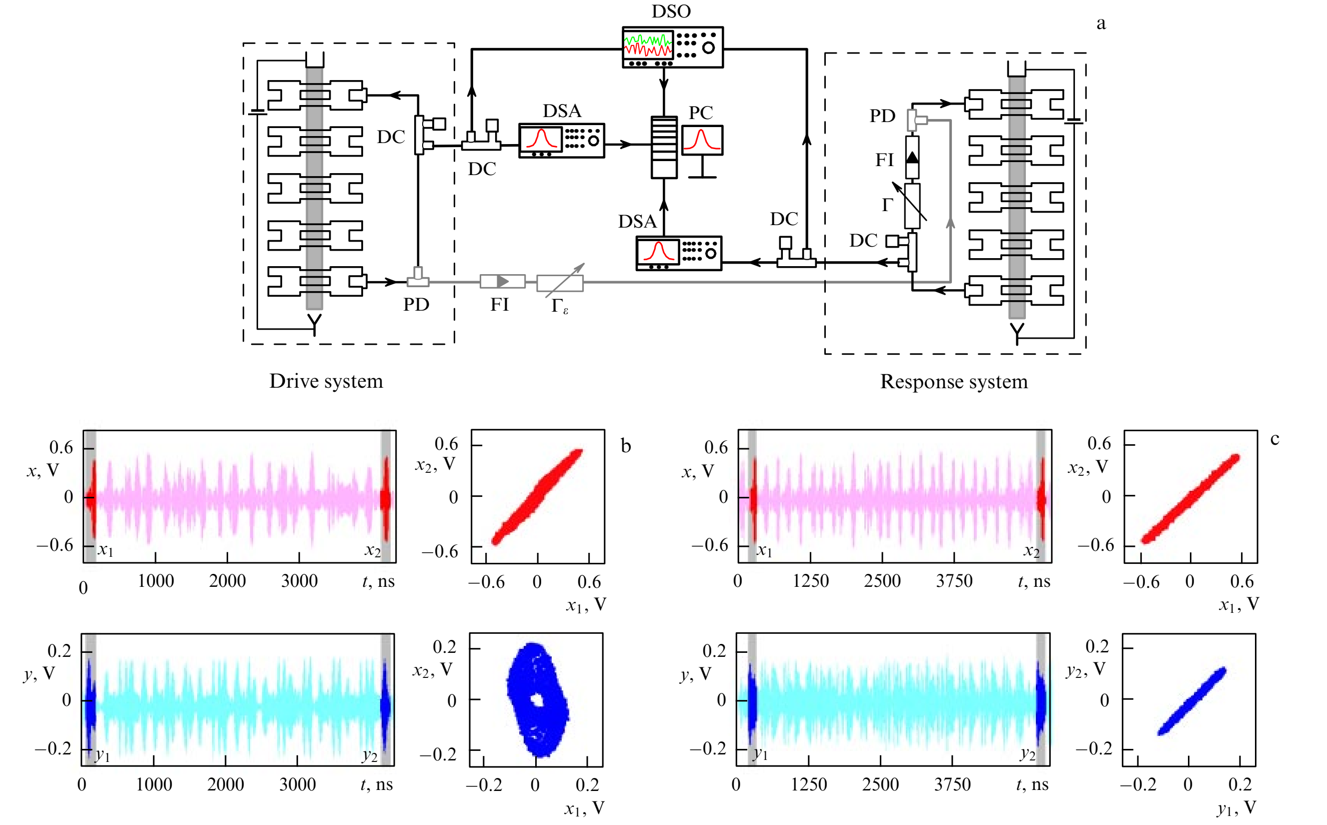

**Figure 18.** (a) Schematic of an experiment on observing generalized synchronization in the microwave range using klystron chaos oscillators with a feedback loop. Dashed-line frames denote klystron chaos oscillators based on five-cavity KY-12 floating drift-tube klystrons with time-delayed feedback. F1 — ferrite isolator, PD — power divider, Γ — waveguide attenuator, DSO — digital HF oscillograph (Agilent Technologies DSO81004B), DSA — digital spectral analyzers, PC — personal computer. (b, c) Distinguished fragments of time series signal outputs from the drive, $x(t)$, and the response, $y(t)$, oscillators and corresponding correlation diagrams $(x_1, x_2)$ and $(y_1, y_2)$ for weak and strong couplings $\varepsilon$ between oscillators: (b) $\varepsilon = 0.1$ (absence of generalized synchronization regime); (c) $\varepsilon = 0.89$ (generalized chaotic synchronization regime). Coupling between the drive and response oscillators was controlled by waveguide attenuator $\Gamma_\varepsilon$ incorporated in the circuit.

telecommunication systems. It should be noted that of all types of chaotic synchronization, generalized synchronization was least studied in experiment, and the main results for it were obtained in the low-frequency range [97, 156], which is of little interest for the purposes of telecommunications. Therefore, the value of this work is restricted to experimental confirmation of the possibility of realizing generalized chaotic synchronization and different methods of its on-line diagnostics.

Thus far, the only work reporting relevant experiments was performed by Dmitriev et al. [199]. It showed the evolvement of generalized chaotic synchronization regime in coupled klystron chaos oscillators operating in centimeter wave range. These oscillators, based on ring-type multicavity klystron amplifiers, stably generate chaotic signals in a wide interval of control parameters [208 – 210]. An experiment with two unidirectionally coupled microwave chaos oscillators is schematically represented in Fig. 18a. The generalized chaotic synchronization regime establishes itself as coupling becomes stronger. An efficient method for its diagnostics in the microwave range, based on the spectral analysis of generated signals, was proposed. The method may find applications in information transmission systems employing generalized chaotic synchronization [199].

Also used for the analysis of synchronization was a modification of the auxiliary system method described in Section 2. The results are presented in Fig. 18b, c showing the experimental time series of output signals of the drive $[x(t)]$ and response $[y(t)]$ oscillators, obtained with an HF digital oscillograph. The 130-ns time interval $T$ chosen for the experiment roughly corresponded to the time delay in the oscillator feedback loop. Thereafter, two time intervals were chosen, $\Delta_1 = (t_1, t_1 + T)$ and $\Delta_2 = (t_2, t_2 + T)$, with similar fragments $x_1(t)$ and $x_2(t)$ of the signal from the drive oscillator $[x_1(t) \approx x_2(t)]$. Fragments of the signal from the response oscillator, $y_1(t)$ and $y_2(t)$, were simultaneously analyzed in the same time intervals. According to the auxiliary system method, the generalized synchronization regime corresponds to the situation in which the states of the response system at time intervals $\Delta_1$ and $\Delta_2$ are close to each other: $y_1(t) \approx y_2(t)$, as illustrated in diagrams $(x_1, x_2)$ and $(y_1, y_2)$ (Fig. 18b, c) for different coupling strengths between the oscillators. Diagrams $(x_1, x_2)$ illustrate the closeness of two selected states of the drive system, and diagrams $(y_1, y_2)$ represent the method for the diagnostics of generalized synchronization. Evidently, in the case of weak coupling, states $y_1(t)$ and $y_2(t)$ of the response oscillator are different at the instants of time when the drive klystron oscillator shows identical dynamics, i.e., there is no functional connection between the states. The situation changes as coupling between unidirectionally coupled oscillators goes stronger; namely, states $y_1(t)$ and $y_2(t)$ become identical as evidenced by the appearance of a diagonal across the plane $(y_1, y_2)$. These findings provide the first experimental confirmation of the possibility of observing generalized synchronization in the microwave range and give reason to suggest the possibility of efficacious diagnostics and, as a consequence, the application of generalized synchronization regimes in modern information transmission and processing systems.

### 7.2 Experiments on information transfer based on chaotic synchronization in the optical range

The discussion in Section 7.1 was focused on important experimental studies of information transmission with the use of chaotic synchronization in the radio frequency and microwave ranges. Today, ring-type optical chaotic oscillators with a laser-based active element are extensively being developed and investigated as having good prospects for practical application [211, Vol. 2, Ch. 4, pp. 353–427]. A number of experiments demonstrated that such devices can be regarded as efficacious easy-to-operate sources of chaotic self-sustained oscillations for information transmission systems [93, 212–216]. Later studies revealed different types of chaotic synchronization in the optical range, including complete, generalized, and phase synchronizations [121, 122, 215, 216–221], and opened up prospects for the application of optical systems as basic elements for information transmission schemes based on the chaotic synchronization phenomenon [222–225].

The very first experiments on signal transfer with the aid of a chaotic carrier demonstrated the operating capacity of schemes based on complete chaotic synchronization [226–229]. A major advantage of such systems operating in the optical range is probably the high information transfer rate (up to 1 Gb $\text{s}^{-1}$) unattainable in other frequency ranges. Complete chaotic synchronization was most extensively used in such experiments, which imposed quite rigorous requirements for noise intensity in the communication channel and parameter mismatch between optical chaos oscillators at both ends of the channel [230]. However, the optical range provides an opportunity for the employment of fiber-optical lines as communication channels due to the low noise and interference level introduced in the transmitted signal; this substantially facilitates the development of operative secure information transfer systems [231]. Moreover, existing commercial fiber-optical communication lines can be used for this purpose.

One example of well-elaborated projects yielding good practical results and aimed at assessing the possibility of using existing commercial fiber-optical lines for long-distance secure communication is the joint study undertaken by a group of researchers from Greece, Spain, Germany, and Belgium. The objective of the study was to achieve a high rate of data transmission over a distance of 120 km via a fiber-optic cable of the Athens metro (Greece) using laser diode-based chaos oscillators [232]. We shall discuss this work at greater length as one of the most successful experimental realizations of information transfer using complete chaotic synchronization in the optical range.

The sources of chaotic signals with a high-dimension attractor and high information entropy were oscillators built around semiconductor diodes with time-delayed feedback realized in two different ways: electrooptical [233], and fully optical [234]. The employment of two types of feedback in the optical chaos oscillator enabled the authors of Ref. [232] to realize two modes of information transfer described above, viz. the nonlinear mixing of the information signal with the chaotic one (Section 3.3), and modulation of the parameters

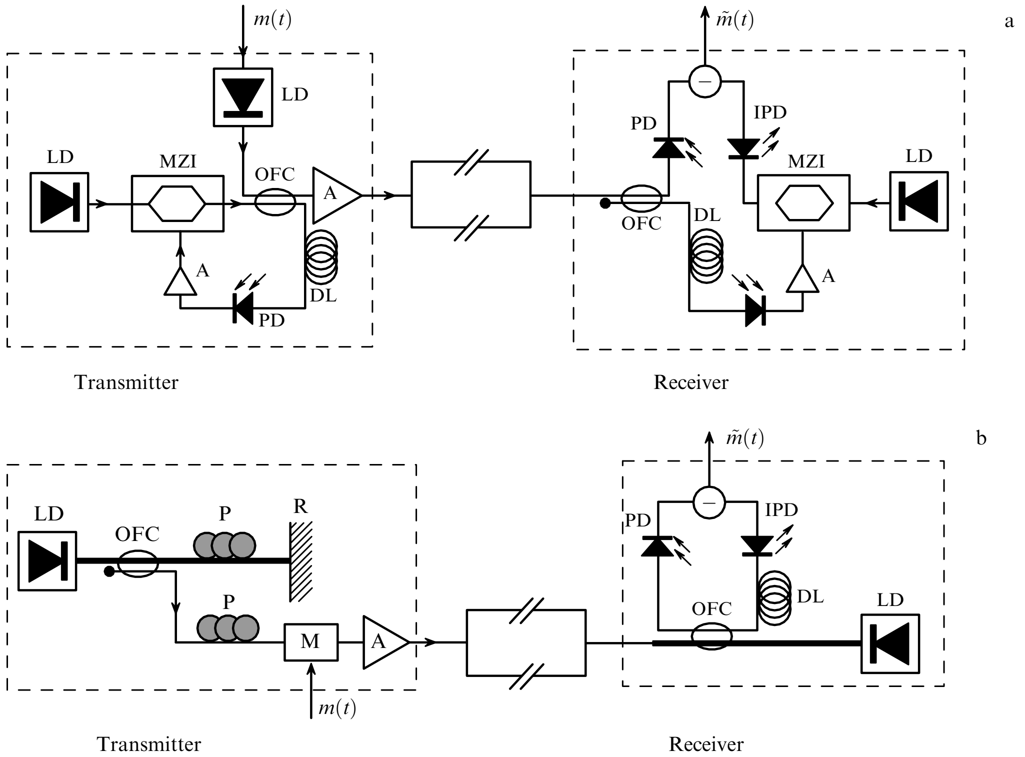

**Figure 19.** Experimental schemes of secure information transmission in the optical range, based on the nonlinear mixing of the information signal with the chaotic one (a) and modulation of parameters of the transmitting oscillator with the information signal (b): LD — laser diode, MZI — Mach–Zehnder electrooptical interferometer, FOM — fiber-optical mixer, R — mirror with variable reflection coefficient, A — amplifier, PD and IPD — photodiodes, DL — delay line, P — polarizer, and M — modulator.

of the chaotic signal with the information signal (Section 3.4). In the former case (see Fig. 19a), radiation emitted by the laser diode (LD) passes through the Mach–Zehnder integrated electrooptical interferometer (MZI) with electrooptical time-delayed feedback (delay line DL, photodiode PD, and electronic amplifier A), which operates as a nonlinear laser radiation modulator. In this case, the information signal is mixed with the feedback signal in fiber-optical mixer (FOM). The output chaotic signal of the oscillator, containing the information message, is additionally amplified before entering the communication channel to achieve the necessary power level. In the latter case (see Fig. 19b), the source of laser radiation is again the laser diode LD, while optical feedback is realized using mirror R whose reflection coefficient nonlinearly depends on incident radiation intensity. The length of the external cavity was 6 m. It contained polarizer P to ensure necessary light polarization after reflection from mirror R with a variable reflection coefficient. The information signal was introduced by way of modulating parameters of the chaotic signal in modulator M. Thereafter, the signal transmitted over the communication channel was amplified as in the former scheme. Both schemes had filters (not shown in Fig. 19) to suppress noise bound up with spontaneous emission [231, 235].

In both schemes, the useful information signal was decoded in the receiver upon establishment of complete chaotic synchronization regime between the oscillators on opposite sides of the communication channel, as discussed at length in Section 3. The main difficulty was the creation of nearly identical oscillators at different ends of the communication channel and the choice of their active elements (semiconductor lasers). Lasers with wavelengths of 1552.0 and 1552.9 nm were utilized in the transmitting and receiving modules, respectively. Each laser operated in an individually chosen temperature regime maintained throughout the experiment to ensure the stable work of laser diodes and identical wavelengths. The choice of highly identical passive elements posed no severe difficulties. Given sufficiently fine adjustment of parameters of optical chaos oscillators, the unidirectionally coupled system was in the stable complete chaotic synchronization regime with a sufficiently powerful signal delivered to the receiver [232]. A parameter mismatch between the oscillators on different sides of the communication channel for the stable operation of the information transmission system (i.e., for achievement of complete chaotic synchronization) should not exceed 3%. Long-distance transmission of the signal created a risk of synchronization destruction as a result of dispersion in the fiber-optical communication channel (it amounted to $-850$ ps nm$^{-1}$ in the experiment under consideration). For this reason, signal feeding to the receiver was preceded by the introduction of fiber-optical fragments with dispersion of opposite sign at the output of the commercial fiber-optical communication line to compensate for dispersive distortion of the signal. Additional amplifiers (not shown in Fig. 19) ensured the desired power.

Figure 20 presents the results of information transfer using a system with electrooptical feedback based on the nonlinear mixing of the information signal with the chaotic one. The information message in the form of a pseudo-random sequence of $2^7 - 1$ bits modulated the chaotic signal as above (Fig. 19a). Figure 20a is an eye pattern (oscillogram of the superposition of a large number of transmitted/received bits) of information signal $m(t)$ (top), transmitted chaotic signal carrying an information message at the transmitter output, and decoded message $m(t)$ in the receiver. The value of BER in this experimental scheme was $10^{-7}$ at an information transmission rate of 3 Gb s$^{-1}$. Similar results were obtained using a scheme with parameter modulation, but the information transmission rate was almost thrice lower ($\sim$ 1 Gb s$^{-1}$) at the same BER value.

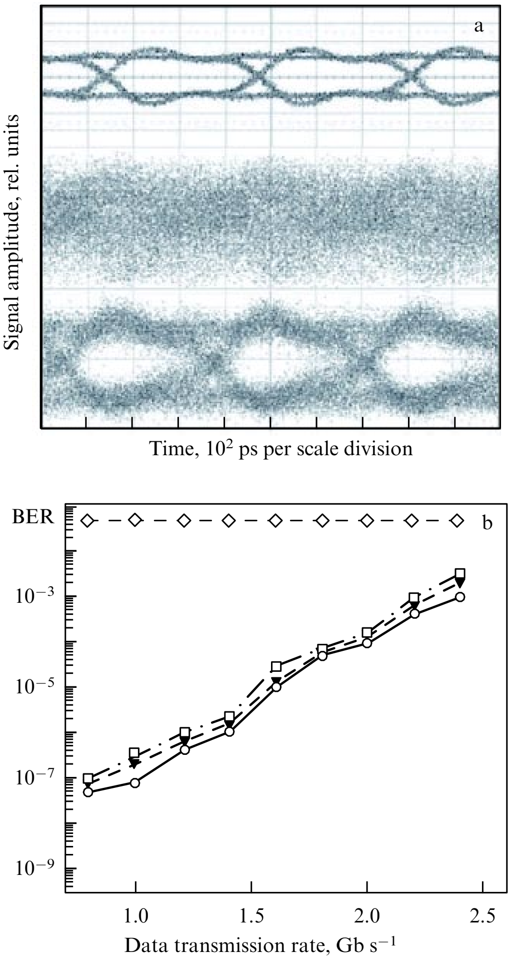

**Figure 20.** (a) Eye patterns of transmitted digital information signal $m(t)$ (top), chaotic signal at the transmitter output (middle), and decoded information message $\tilde{m}(t)$ at the receiver output (bottom) using a scheme of the nonlinear mixing of the information signal with the chaotic one. (b) Dependence of bit error rate (BER) on information transmission rate using a scheme with modulation of parameters of the transmitting oscillator: ◇ — results of an analysis of the coded message at the output of the transmitting module; ○ — results of a laboratory experiment on short-distance information transmission; ▼ — results of an experiment on long-distance ($\sim$ 120 km) transmission of a short information message ($2^7 - 1$) over a commercial fiber-optic line, and □ — results of an experiment on long-distance transmission of a $2^{23} - 1$-long information message. (Taken from Ref. [232].)

Bearing in mind the importance of the stability of chaotic synchronization-based information transmission systems under the effect of different factors, it appears appropriate to discuss the quality of information transfer, which is convenient to describe in this experiment by the bit error rate at a varying rate of information transmission. Its decrease lengthens the time needed to transfer a single bit and thereby significantly facilitates the on-line diagnostics of the receiver state for reliable reception of the message. The authors of Ref. [232] carried out studies at different information transmission rates, from 0.1 to 2.4 Gb s$^{-1}$, for two lengths of transmitted pseudorandom bit sequences: $2^7-1$ and $2^{23}-1$. Figure 20b shows the dependences of BER on the information transmission rate using a scheme with parameter modulation (Fig. 19b). Evidently, transmission quality decreases with increasing transmission rate. The chaotic signal is adequately encoded (see the curve marked by diamonds), but the nonidentity of oscillators, noise in the oscillators and communication channel begin to exert destructive action and restrict the information transmission rate. The error was unrelated to the distance over which the data were transferred. It means that the main limitations on the method dictated by the quality (i.e., high transmission rate) requirement are related to the nonidentity of the oscillators on opposite sides of the communication channel and fluctuations in the oscillators.

The results obtained in Ref. [232] are of paramount importance and open up good prospects for the application of information transmission schemes using chaotic synchronization in the optical range in modern information–telecommunication systems. These studies were carried out based on commercial telecommunication networks, which means that practical application of the technologies of interest does not require replacement of the existing equipment. A disadvantage of these schemes is the relatively low rate of data transmission; it is shared by all other similar secure data transmission systems that depend on the achievement of complete chaotic synchronization regimes highly sensitive to the detuning of chaos oscillators on different sides of the communication channel and noise always present in real experiments.

## 8. Conclusions

The present review focused on secure communication methods with the use of chaotic signals. These methods employ different types of synchronous behavior of chaotic systems, such as complete chaotic synchronization, phase synchronization, generalized chaotic synchronization, or several types of such behavior at a time (e.g., generalized and complete synchronization). Each scheme displays specific features, merits and demerits and operates on its own principles. At the same time, most of them have common drawbacks and share the difficulties of practical realization arising from the necessity of (1) close identity between oscillators on opposite sides of the communication channel, (2) low robustness against intrachannel noise, and (3) rather low degree of confidentiality.

Much attention was given to a method of secure information transmission based on generalized chaotic synchronization free of these disadvantages. All the methods considered were compared by numerically simulating unidirectionally coupled chaotic Rössler systems selected for transmitting and receiving oscillators

An analysis of the quantitative characteristics of the operating capacity of secure communication systems revealed that the method based on generalized chaotic synchronization shows practically unlimited stability under real conditions of noisy communication channels, in contrast to all other schemes. Moreover, it is robust against parameter mismatch between initially identical chaos oscillators located on one side of the communication channel (an important advantage) and against nonlinear distortions in the channel.

This method opens up new opportunities for the experimental realization of secure communication using chaotic synchronization. The absence of many drawbacks inherent in other secure communication techniques makes further improvement of this method a challenging problem.

This review of the experimental realization of different secure communication methods focuses on chaotic masking, nonlinear mixing, and modulation of control parameters in the radio frequency, microwave, and optical ranges. Preliminary results of experimental studies on the generalized chaotic synchronization regime in the microwave range are presented.

The authors are grateful to A S Dmitriev and D I Trubetskov for enlightening discussions and constructive criticism. The valuable comments of the reviewer are acknowledged. The work was supported by RFBR (project 08-02-00102), the President's Programs for Support of Leading Scientific Schools (project NSh-355.2008.2), 'Nonlinear Dynamics and Biophysics' Research and Educational Centre, Saratov State University (CRDF REC-006), sectoral analytical target program Development of the Research Potential of Higher Schools, and the Federal Target Program 'Academic and Teaching Staff of an Innovative Russia' for 2009–2013.

## References

1. Huygens C *Horologium Oscillatorium, Sive de Motu Pendulorum ad Horologia Aptato Demonstrationes Geometrical* (Paris: A.F. Muguet, 1673) [Translated into English: *The Pendulum Clock or, Geometrical Demonstrations Concepting the Motion of Pendula as Applied to Clocks* (Ames: Iowa State Univ. Press, 1986)]
2. Van der Pol B *Proc. IRE* **22** 1051 (1934) [Translated into Russian: *Nelineinaya Teoriya Elektricheskikh Kolebanii* (Moscow: Svyaz'tekhizdat, 1935)]
3. Gaponov V I *Zh. Tekh. Fiz.* **6** 801 (1936)
4. Teodorchik K F *Dokl. Akad. Nauk SSSR* **40** (2) 63 (1943)
5. Adler R *Proc. IRE* **34** (6) 351 (1946); reprinted: *Proc IEEE* **61** 1380 (1973)
6. Khokhlov R V *Dokl. Akad. Nauk SSSR* **97** 411 (1954)
7. Andronov A A, Vitt A A, in Andronov A A *Sobranie Trudov* (Collective Works) (Moscow: Izd. AN SSSR, 1956)
8. Minakova I I, Teodorchik K F *Dokl. Akad. Nauk SSSR* **106** 658 (1956)
9. Andronov A A, Vitt A A, Khaikin S E *Teoriya Kolebanii* (Theory of Oscillations) (Moscow: Nauka, 1981) [Translated into English (New York: Dover, 1987)]
10. Blekhman I I *Sinkhronizatsiya Dinamicheskikh Sistem* (Synchronization of Dynamical Systems) (Moscow: Nauka, 1971)
11. Blekhman I I *Sinkhronizatsiya v Prirode i Tekhnike* (Synchronization in Science and Technology) (Moscow: Nauka, 1981) [Translated into English (New York: ASME Press, 1988)]
12. Anishchenko V S, Vadivasova T E, Astakhov V V *Nelineinaya Dinamika Khaoticheskikh i Stokhasticheskikh Sistem. Fundamental'nye Osnovy i Izbrannye Problemy* (Non-Linear Dynamics of Chaotic and Stochastic Systems. Fundamentals and Selected Problems) (Saratov: Izd. Sarat. Univ., 1999)
13. Anishchenko V S et al. *Nelineinye Effekty v Khaoticheskikh i Stokhasticheskikh Sistemakh* (Ed. V S Anishchenko) (Non-Linear Effects in Chaotic and Stochastic Systems) (Moscow–Izhevsk: Inst. Komp'yut. Issled., 2003)
14. Pikovskii A S, Rozenblum M G, Kurts Yu *Sinkhronizatsiya. Fundamental'noe Nelineinoe Yavlenie* (Synchronization. A Fundamental Non-Linear Phenomenon) (Moscow: Tekhnosfera, 2003)
15. Trubetskov D I *Sinkhronizatsiya*: *Uchenyi i Vremya* (Synchronization: The Researcher and the Time) (Saratov: Izd. GosUNTs 'Kolledzh', 2005) p. 70
16. Anishchenko V S et al. *Sinkhronizatsiya Regulyarnykh Khaoticheskikh i Stokhasticheskikh Kolebanii* (Synchronization of Regular Chaotic and Stochastic Oscillations) (Moscow – Izhevsk: RKhD, 2008)

17. Anishchenko V S, Astakhov V V, Letchford T E *Radiotekh. Elektron.* **27** 1972 (1980)
18. Kuznetsov Yu I et al. *Dokl. Akad. Nauk SSSR* **275** 1388 (1984) [*Sov. Phys. Dokl.* **29** 318 (1984)]
19. Dmitriev A S, Kislov V Ya, Starkov S O *Zh. Tekh. Fiz.* **55** 2417 (1985) [*Sov. Phys. Tech. Phys.* **30** 1439 (1985)]
20. Afraimovich V S, Verichev N N, Rabinovich M I *Izv. Vyssh. Uchebn. Zaved, Radiofiz.* **29** 1050 (1986) [*Radiophys. Quantum Electron.* **29** 795 (1986)]
21. Neimark Yu I, Landa P S *Stokhasticheskie i Khaoticheskie Kolebaniya* (Stochastic and Chaotic Oscillations (Moscow: Nauka, 1987) [Translated into English (Dordrecht: Kluwer Acad. Publ., 1992)]
22. Anishchenko V S *Sloznye Kolebaniya v Prostykh Sistemakh* (Complicated Oscillations in Simple Systems) (Moscow: Nauka, 1990)
23. Dmitriev A S, Panas A I *Dinamicheskii Khaos: Novye Nositeli Informatsii dlya Sistem Svyazi* (Dynamical Chaos: New Information Carriers for Communication Systems) (Moscow: Fizmatlit, 2002)
24. Parlitz U et al. *Int. J. Bifurcat. Chaos* **2** 973 (1992)
25. Cuomo K M, Oppenheim A V, Strogatz S H *IEEE Trans. Circuits Syst. II Analog Digital Signal Process.* **40** 626 (1993)
26. Kocarev L, Parlitz U *Phys. Rev. Lett.* **74** 5028 (1995)
27. Peng J H, Ding E J, Ding M, Yang W *Phys. Rev. Lett.* **76** 904 (1996)
28. Anishchenko V S, Pavlov A N *Phys. Rev. E* **57** 2455 (1998)
29. Anishchenko V S, Pavlov A N, Yanson N B *Zh. Tekh. Fiz.* **68** (12) 1 (1998) [*Tech. Phys.* **43** 1401 (1998)]
30. Eguia M C, Rabinovich M I, Abarbanel H D I *Phys. Rev. E* **62** 7111 (2000)
31. Fischer I, Liu Y, Davis P *Phys. Rev. A* **62** 011801 (2000)
32. Rulkov N F, Vorontsov M A, Illing L *Phys. Rev. Lett.* **89** 277905 (2002)
33. Yuan Z L, Shields A J *Phys. Rev. Lett.* **94** 048901 (2005)
34. Li Q S, Liu Y *Phys. Rev. E* **73** 016218 (2006)
35. Fradkov A L, Andrievsky B, Evans R J *Phys. Rev. E* **73** 066209 (2006)
36. Strogatz S H *Nonlinear Dynamics and Chaos: with Applications to Physics, Biology, Chemistry, and Engineering* (Reading, Mass.: Addison-Wesley, 1994)
37. Elson R C et al. *Phys. Rev. Lett.* **81** 5692 (1998)
38. Landa P S, Rabinovitch A *Phys. Rev. E* **61** 1829 (2000)
39. Porcher R, Thomas G *Phys. Rev. E* **64** 010902 (2001)
40. Glass L *Nature* **410** 277 (2001)
41. Pavlov A N et al. *Physica A* **316** 233 (2002)
42. Sosnovtseva O V et al. *Phys. Rev. E* **66** 061909 (2002)
43. Rosenblum M G, Pikovsky A S, Kurths J *Fluctuat. Noise Lett.* **4** L53 (2004)
44. Postnov D E, Khan S K *Pis'ma Zh. Tekh. Fiz.* **25** (4) 11 (1999) [ *Tech. Phys. Lett.* **25** 128 (1999)]
45. Anishchenko V S et al. *Int. J. Bifurcat. Chaos* **10** 2339 (2000)
46. Mosekilde E, Maistrenko Y, Postnov D *Chaotic Synchronization: Applications to Living Systems* (River Edge, NJ: World Scientific, 2002)
47. Prokhorov M D et al. *Phys. Rev. E* **68** 041913 (2003)
48. Rulkov N F *Phys. Rev. E* **65** 041922 (2002)
49. Sosnovtseva O V et al. *Izv. Vyssh. Ucheb. Zaved. Priklad. Nelinein. Din.* **11** (3) 133 (2003)
50. Sosnovtseva O V et al. *Phys. Rev. E* **70** 031915 (2004)
51. Sosnovtseva O V et al. *Physiol. Meas.* **26** 351 (2005)
52. Sosnovtseva O V et al. *Phys. Rev. Lett.* **94** 218103 (2005)
53. Hramov A E et al. *Phys. Rev. E* **73** 026208 (2006)
54. Sosnovtseva O V et al. *Am. J. Physiol. Renal Physiol.* **293** F1545 (2007)
55. Parmananda P *Phys. Rev. E* **56** 1595 (1997)
56. Kiss I Z, Hudson J L *Phys. Rev. E* **64** 046215 (2001)
57. Rosenblum M, Pikovsky A *Contemp. Phys.* **44** 401 (2003)
58. Kiss I Z et al. *Phys. Rev. E* **70** 026210 (2004)
59. Yoshioka M *Phys. Rev. E* **71** 061914 (2005)
60. Ditto W L, Rauseo S N, Spano M L *Phys. Rev. Lett.* **65** 3211 (1990)
61. Meucci R et al. *Phys. Rev. E* **49** R2528 (1994)
62. Kittel A, Parisi J, Pyragas K *Phys. Lett. A* **198** 433 (1995)
63. Shalfeev V D et al. *Zarubezh. Radioelektron. Usp. Sovremen. Radioelektron.* (10) 27 (1997)
64. Boccaletti S et al. *Phys. Rep.* **329** 103 (2000)
65. Ticos C M et al. *Phys. Rev. Lett.* **85** 2929 (2000)
66. Rosa E (Jr.) et al. *Int. J. Bifurcat. Chaos* **10** 2551 (2000)
67. Trubetskov D I, Khramov A E *Radiotekh. Elektron.* **48** 116 (2003) [*J. Commun. Technol. Electron.* **48** 105 (2003)]
68. Trubetskov D I, Koronovsky A A, Khramov A E *Izv. Vyssh. Ucheb. Zaved. Radiofiz.* **47** 343 (2004) [*Radiophys. Quantum Electron.* **47** 305 (2004)]
69. Hramov A E et al. *Chaos* **15** 013705 (2005)
70. Beloglazkina M V, Koronovskii A A, Hramov A E *Zh. Tekh. Fiz.* **79** (6) 13 (2009) [*Tech. Phys.* **54** 775 (2009)]
71. Fradkov A L *Usp. Fiz. Nauk* **175** 113 (2005) [*Phys. Usp.* **48** 103 (2005)]
72. Abarbanel H D I et al. *Usp. Fiz. Nauk* **166** 363 (1996) [*Phys. Usp.* **39** 337 (1996)]
73. Bezruchko B P et al. *Usp. Fiz. Nauk* **178** 323 (2008) [*Phys. Usp.* **51** 304 (2008)]
74. Tass P et al. *Phys. Rev. Lett.* **81** 3291 (1998)
75. Tass P A et al. *Phys. Rev. Lett.* **90** 088101 (2003)
76. Meinecke F C et al. *Phys. Rev. Lett.* **94** 084102 (2005)
77. Chavez M et al. *Chaos* **15** 023904 (2005)
78. Yang T *Int. J. Computat. Cognition* **2** (2) 81 (2004)
79. Tang Y, Fang J, Chen L *Int. J. Mod. Phys. B* **22** 4175 (2008)
80. Zheng G, Boutat D, Floquet T, Barbot J-P *Int. J. Bifurcat. Chaos* **18** 2063 (2008)
81. Bowong S, Yamapi R *Int. J. Bifurcat. Chaos* **18** 2425 (2008)
82. Hoang T M, Nakagawa M *Chaos, Solitons Fractals* **38** 1423 (2008)
83. Liang X, Zhang J, Xia X *IEEE Trans. Circuits Syst. II Express Briefs* **55** 680 (2008)
84. Wang X et al. *Mod. Phys. Lett. B* **22** 2077 (2008)
85. Tronciu V Z et al. *Opt. Commun.* **281** 4747 (2008)
86. Gámez-Guzmán L et al. *Rev. Mex. Fís.* **54** (4) 299 (2008)
87. Sun Y, Cao J, Feng G *Phys. Lett. A* **372** 5442 (2008)
88. Wang Yun-Cai, Zhao Qing-Chun, Wang An-Bang *Chinese Phys. B* **17** 2373 (2008)
89. Yu W, Cao J, Yuan K *Phys. Lett. A* **372** 4438 (2008)
90. Materassi D, Basso M *Int. J. Bifurcat. Chaos* **18** 567 (2008)
91. Xia W, Cao J *Chaos* **18** 023128 (2008)
92. Lu S, Chen L *Kybernetika* **44** (1) 43 (2008)
93. Annovazzi-Lodi V et al. *IEEE Photonics Technol. Lett.* **17** 1995 (2005)
94. Pecora L M, Carroll T L *Phys. Rev. Lett.* **64** 821 (1990)
95. Pecora L M, Carroll T L *Phys. Rev. A* **44** 2374 (1991)
96. Rosenblum M G, Pikovsky A S, Kurths J *Phys. Rev. Lett.* **76** 1804 (1996)
97. Rulkov N F et al. *Phys. Rev. E* **51** 980 (1995)
98. Rosenblum M G, Pikovsky A S, Kurths J *Phys. Rev. Lett.* **78** 4193 (1997)
99. Fahy S, Hamann D R *Phys. Rev. Lett.* **69** 761 (1992)
100. Martian A, Banavar J R *Phys. Rev. Lett.* **72** 1451 (1994)
101. Kaulakys B, Vektaris G *Phys. Rev. E* **52** 2091 (1995)
102. Chen Y-Y *Phys. Rev. Lett.* **77** 4318 (1996)
103. Kaulakys B, Ivanauskas F, Meškauskas T *Int. J. Bifurcat. Chaos* **9** 533 (1999)
104. Toral R et al. *Chaos* **11** 665 (2001)
105. Gribunin V G, Okov I N, Turintsev I V *Tsifrovaya Steganografiya* (Digital Steganography) (Moscow: SOLON-Press, 2002)
106. Murali K, Lakshmanan M *Phys. Rev. E* **48** R1624 (1993)
107. Boccaletti S, Farini A, Arecchi F T *Phys. Rev. E* **55** 4979 (1997)
108. Carroll T L, Johnson G A *Phys. Rev. E* **57** 1555 (1998)
109. Terry J R, Van Wiggeren G D *Chaos, Solitons Fractals* **12** 145 (2001)
110. Lucamarini M, Mancini S *Phys. Rev. Lett.* **94** 140501 (2005)
111. Eckmann J-P, Thomas L, Wittwer P *J. Phys. A* **14** 3153 (1981)
112. Kye W-H, Kim C-M *Phys. Rev. E* **62** 6304 (2000)
113. Kye W-H et al. *Phys. Rev. E* **68** 036203 (2003)
114. Hramov A E et al. *Phys. Rev. E* **76** 026206 (2007)
115. Koronovskii A A, Hramov A E *Eur. Phys. J. B* **62** 447 (2008)
116. Pikovsky A S, Kurths J *Phys. Rev. Lett.* **78** 775 (1997)
117. Mangioni S et al. *Phys. Rev. Lett.* **79** 2389 (1997)
118. Zaikin A A, Kurths J, Schimansky-Geier L *Phys. Rev. Lett.* **85** 227 (2000)
119. Neiman A B, Russell D F *Phys. Rev. Lett.* **88** 138103 (2002)
120. Zhou C et al. *Phys. Rev. Lett.* **89** 014101 (2002)

121. Zhou C S et al. *Phys. Rev. E* **67** 015205 (2003)
122. Boccaletti S et al. *Phys. Rev. Lett.* **89** 194101 (2002)
123. Taherion S, Lai Y-C *Phys. Rev. E* **59** R6247 (1999)
124. Boccaletti S et al. *Phys. Rep.* **366** 1 (2002)
125. Volkovskii A R, Rul'kov N F *Pis'ma Zh. Tekh. Fiz.* **19** (3) 71 (1993) [*Tech. Phys. Lett.* **19** 97 (1993)]
126. Pyragas K *Phys. Rev. E* **54** R4508 (1996)
127. Pecora L M, Carroll T L, Heagy J F *Phys. Rev. E* **52** 3420 (1995)
128. Pyragas K *Phys. Rev. E* **56** 5183 (1997)
129. Abarbanel H D I, Rulkov N F, Sushchik M M *Phys. Rev. E* **53** 4528 (1996)
130. Osipov G V et al. *Phys. Rev. E* **55** 2353 (1997)
131. Pikovsky A, Rosenblum M, Kurths J *Int. J. Bifurcat. Chaos* **10** 2291 (2000)
132. Rosenblum M G et al., in *Nonlinear Analysis of Physiological Data* (Eds H Kantz, J Kurths, G Mayer-Kress) (Berlin: Springer, 1998) p. 91
133. Vadivasova T E, Anishchenko V S *Radiotekh. Elektron.* **49** 77 (2004) [*J. Commun. Technol. Electron.* **49** 69 (2004)]
134. Pikovsky A S et al. *Physica D* **104** 219 (1997)
135. Pikovsky A, Rosenblum M, Kurths J *Synchronization: A Universal Concept in Nonlinear Sciences* (Cambridge: Cambridge Univ. Press, 2001)
136. Anishchenko V S, Vadivasova T E, Strelkova G I *Fluctuat. Noise Lett.* **4** L219 (2004)
137. Pikovsky A S, Rosenblum M G, Kurths J *Europhys. Lett.* **34** 165 (1996)
138. Koronovskii A A, Hramov A E, Hramova A E *Pis'ma Zh. Eksp. Teor. Fiz.* **82** 176 (2005) [*JETP Lett.* **82** 160 (2005)]
139. Rosenblum M G et al. *Phys. Rev. Lett.* **89** 264102 (2002)
140. Hramov A E, Koronovskii A A *Chaos* **14** 603 (2004)
141. Hramov A E, Koronovskii A A, Levin Yu I *Zh. Eksp. Teor. Fiz.* **127** 886 (2005) [*JETP* **100** 784 (2005)]
142. Koronovskii A A, Kurovskaya M K, Hramov A E *Pis'ma Zh. Tekh. Fiz.* **31** (19) 76 (2005) [*Tech. Phys. Lett.* **31** 847 (2005)]
143. Koronovskii A A, Khramov A E *Radiotekh. Elektron.* **50** 969 (2005) [*J. Commun. Technol. Electron.* **50** 894 (2005)]
144. Hramov A E, Koronovskii A A *Physica D* **206** 252 (2005)
145. Dedieu H, Kennedy M P, Hasler M *IEEE Trans. Circuits Syst. I Regular Papers* **40** 634 (1993)
146. Dmitriev A S, Panas A I, Starkov S O *Int. J. Bifurcat. Chaos* **5** 1249 (1995)
147. Yang T, Chua L O *IEEE Trans. Circuits Syst. I Regular Papers* **43** 817 (1996)
148. Downes P T *SPIE* **2038** 227 (1993)
149. Pérez G, Cerdeira H A *Phys. Rev. Lett.* **74** 1970 (1995)
150. Short K M *Int. J. Bifurcat. Chaos* **6** 367 (1996)
151. Ponomarenko V I, Prokhorov M D *Phys. Rev. E* **66** 026215 (2002)
152. Koronovskii A A et al. *Dokl. Ross. Akad. Nauk* **383** 322 (2002) [*Dokl. Phys.* **47** 181 (2002)]
153. Koronovsky A A et al. *Izv. Vyssh. Uchebn. Zaved. Radiofiz.* **45** 880 (2002) [*Radiophys. Quantum Electron.* **45** 806 (2002)]
154. Yang T *Int. J. Circuit Theory Appl.* **23** 611 (1995)
155. Chen J Y et al. *Chaos* **13** 508 (2003)
156. Rulkov N F *Chaos* **6** 262 (1996)
157. Zheng Z, Hu G *Phys. Rev. E* **62** 7882 (2000)
158. Hramov A E, Koronovskii A A, Moskalenko O I *Europhys. Lett.* **72** 901 (2005)
159. Koronovskii A A, Popov P V, Hramov A E *Zh. Eksp. Teor. Fiz.* **130** 748 (2006) [*JETP* **103** 654 (2006)]
160. Moskalenko O I et al. *Phys. Rev. E* (2009), submitted
161. Murali K, Lakshmanan M *Phys. Lett. A* **241** 303 (1998)
162. Koronovskii A A et al. *Izv. Ross. Akad. Nauk. Fiz.* **72** (1) 143 (2008) [*Bull. Russ. Acad. Sci. Phys.* **72** 131 (2008)]
163. Koronovskii A et al. *Pervaya Milya* (1) 14 (2008)
164. Koronovskii A A, Moskalenko O I, Hramov A E *Zh. Tekh. Fiz.* **76** (2) 1 ( 2006) [*Tech. Phys.* **51** 143 (2006)]
165. Hramov A E, Koronovskii A A *Phys. Rev. E* **71** 067201 (2005)
166. Koronovskii A A et al. *Izv. Ross. Akad. Nauk. Fiz.* **73** 1723 (2009)
167. Koronovskii A A, Hramov A E *Pis'ma Zh. Eksp. Teor. Fiz.* **79** 391 (2004) [*JETP Lett.* **79** 316 (2004)]
168. Koronovskii A A, Moskalenko O I, Hramov A E *Pis'ma Zh. Eksp. Teor. Fiz.* **80** 25 (2004) [*JETP Lett.* **80** 20 (2004)]
169. Koronovskii A A, Moskalenko O I, Hramov A E *Radiotekh. Elektron.* **52** 949 (2007) [*J. Commun. Technol. Electron.* **52** 881 (2007)]
170. Rico-Martínez R et al. *Physica D* **176** 1 (2003)
171. Nikitin N N, Pervachev S V, Razevig V D *Avtomatika Telemekh.* (4) 133 (1975)
172. Sklar B *Digital Communications. Fundamentals and Applications* (Upper Saddle River, NJ: Prentice-Hall PTR, 2001) [Translated into Russian (Moscow: Vil'yams, 2003)]
173. Poberezhskii E S *Tsifrovye Radiopriemnye Ustroistva* (Digital Radio Receivers) (Moscow: Radio i Svyaz', 1987)
174. Abel A, Schwarz W *Proc. IEEE* **90** 691 (2002)
175. Chua L O *Arch. Elektron. Übertragungstech.* **46** 250 (1992)
176. Chua L O, Komuro M, Matsumoto T *IEEE Trans. Circuits Syst.* **CAS-33** 1073 (1986)
177. Kuznetsov S P *Izv. Vyssh. Ucheb. Zaved. Radiofiz.* **25** 1410 (1982) [*Radiophys. Quantum Electron.* **25** 996 (1982)]
178. Dmitriev A S, Panas A I, Starkov S O *Int. J. Bifurcat. Chaos* **6** 851 (1996)
179. Hramov A E et al. *Phys. Rev. E* **75** 056207 (2007)
180. Ponomarenko V P, Matrosov V V *Radiotekh. Elektron.* **29** 1125 (1984)
181. Kapranov M V, Chernobaev V G *Radiotekh. Tetradi* (15) 86 (1998)
182. Shalfeev V D, Matrosov V V, Korzinova M V *Zarubezh. Radioelektron. Usp. Sovremen. Radioelektron.* (11) 44 (1998)
183. Matrosov V V, Shalfeev V D, Kasatkin D V *Izv. Vyssh. Ucheb. Zaved. Radiofiz.* **49** 448 (2006) [*Radiophys. Quantum Electron.* **49** 406 (2006)]
184. Bel'skii Yu L et al. *Radiotekh. Elektron.* **37** 660 (1992)
185. Ott E, Sommerer J C *Phys. Lett. A* **188** 39 (1994)
186. Boccaletti S, Valladares D L *Phys. Rev. E* **62** 7497 (2000)
187. Hramov A E, Koronovskii A A *Europhys. Lett.* **70** 169 (2005)
188. Lai Y-C *Phys. Rev. E* **53** R4267 (1996)
189. Cuomo K M, Oppenheim A V *Phys. Rev. Lett.* **71** 65 (1993)
190. Dmitriev A S et al. *Radiotekh. Elektron.* **43** 1115 (1998) [*J. Commun. Technol. Electron.* **43** 1038 (1998)]
191. Matsumoto T *IEEE Trans. Circuits Systems* **31** 1055 (1984)
192. Zhong G-Q, Ayrom F *Int. J. Circuit Theory Appl.* **13** 93 (1985)
193. Dmitriev A S, Panas A I, Kuzmin L V *Nonlinear Phenom. Complex Syst.* **2** (3) 91 (1999)
194. Panas A I, Yang T, Chua L O *Int. J. Bifurcat. Chaos* **8** 639 (1998)
195. Panas A I, in *Proc. of the 6th Intern. Workshop NDES'98, Budapest, Hungary, 1998*, p. 257
196. Kuz'min L V, Maksimov N A, Panas A *Izv. Vyssh. Uchebn. Zaved. Priklad. Nelin. Dinamika* **7** (2–3) 81 (1999)
197. Emets S V, Starkov S O *Izv. Vyssh. Uchebn. Zaved. Priklad. Nelin. Dinamika* **7** (2–3) 95 (1999)
198. Larsen P B, Earley L M, Wheat R M, Booske J H, in *Proc. of Vacuum Electronics Conf., 2006, Jointly with 2006 IEEE International Vacuum Electron. Sources, IEEE Intern.* (2006) p. 521
199. Dmitriev A S et al. *Phys. Rev. Lett.* **102** 074101 (2009)
200. Marchewka C et al. *Phys. Plasmas* **13** 013104 (2006)
201. Kislov V Ya, Myasin V E, Bogdanov E V "Generator SVCh shirokopolosnykh kolebaniy" ("Broadband microwave oscillator"), Application No. 984513/19-09 of 31.07.68
202. Kislov V Ya, Zalogin N N, Myasin E A *Radiotekh. Elektron.* **24** 1118 (1979)
203. Kislov V Ya, Myasin E A, Zalogin N N *Radiotekh. Elektron.* **25** 2160 (1980)
204. Kats V A, Trubetskov D I *Pis'ma Zh. Eksp. Teor. Fiz.* **39** (3) 116 (1984) [*JETP Lett.* **39** 137 (1984)]
205. Trubetskov D I, Hramov A E *Lektsii po Sverkhvysokochastotnoi Elektronike dlya Fizikov* (Lectures on Microwave Electronics for Physicists) Vol. 2 (Moscow: Fizmatlit, 2004)
206. Ryskin N M et al. *Phys. Plasmas* **11** 1194 (2004)
207. Dronov V et al. *Chaos* **14** 30 (2004)
208. Koronovskii A A et al. *Obobshchennaya Khaoticheskaya Sinkhronizatsiya v Diapazone Sverkhvysokikh Chastot* (Generalized Chaotic Synchronization in the Microwave Range) Vol. 2 (Moscow: Fizmatlit, 2008) Ch. 9
209. Shigaev A M et al. *IEEE Trans. Electron Dev.* **52** 790 (2005)

210. Trubetskov D I, Hramov A E *Lektsii po Sverkhvysokochastotnoi Elektronike dlya Fizikov* (Lectures on Microwave Electronics for Physicists) Vol. 1 (Moscow: Fizmatlit, 2003)
211. Evans M W (Ed.) *Modern Nonlinear Optics* (Adv. in Chem. Phys., Vol. 119, Pt. 3, Eds I Prigogine, S A Rice) Vols 1 – 3, 2nd ed. (New York: Wiley, 2001)
212. Udaltsov V S et al. *IEEE Trans. Circuits Syst. I Fundament. Theory Appl.* **49** 1006 (2002)
213. Uchida A et al., in *Papers of Technical Meeting on Optical and Quantum Devices, IEE Japan OQD-01* (37 – 46) 1 (2001)
214. Matsuura T, Uchida A, Yoshimori S *Opt. Lett.* **29** 2731 (2004)
215. Yamamoto T et al. *Opt. Express* **15** 3974 (2007)
216. Uchida A, Ogawa T, Kannari F *Jpn. J. Appl. Phys.* **37** L730 (1998)
217. McAllister R et al. *Physica D* **195** 244 (2004)
218. Uchida A et al. *Opt. Lett.* **24** 890 (1999)
219. Soriano M et al. *Phys. Rev. E* **78** 046218 (2008)
220. Uchida A et al. *Phys. Rev. E* **68** 016215 (2003)
221. Ruiz-Oliveras F R, Pisarchik A N *Phys. Rev. E* **79** 016202 (2009)
222. Chlouverakis K E et al. *Physica D* **237** 568 (2008)
223. Argyris A et al. *IEEE J. Select. Top. Quantum Electron.* **10** 927 (2004)
224. Argyris A, Syvridis D *J. Lightwave Technol.* **22** 1272 (2004)
225. Uchida A, Liu Y, Davis P *IEEE J. Quantum Electron.* **39** 963 (2003)
226. Tang S, Liu J *Opt. Lett.* **26** 1843 (2001)
227. Liu J M, Chen H F, Tang S *IEEE Trans. Circuits Systems I Fundament. Theory Appl.* **48** 1475 (2001)
228. Kusumoto K, Ohtsubo J *Opt. Lett.* **27** 989 (2002)
229. Abarbanel H D I et al. *IEEE J. Quantum Electron.* **37** 1301 (2001)
230. Bogris A, Argyris A, Syvridis D *IEEE J. Quantum Electron.* **43** 552 (2007)
231. Lee M W, Larger L, Goedgebuer J-P *IEEE J. Quantum Electron.* **39** 931 (2003)
232. Argyris A et al. *Nature* **438** 343 (2005)
233. Goedgebuer J-P, Larger L, Porte H *Phys. Rev. Lett.* **80** 2249 (1998)
234. Van Wiggeren G D, Roy R *Science* **279** 1198 (1998)
235. Paul J, Lee M W, Shore K A *Opt. Lett.* **29** 2497 (2004)