Breaking a secure communication scheme based on the phase synchronization of chaotic systems

G. Álvarez,[a] F. Montoya, G. Pastor, and M. Romera
Instituto Física Aplicada, Consejo Superior de Investigaciones Científicas, Serrano 144, 28006-Madrid, Spain

(Received 17 November 2003; accepted 30 January 2004; published online 11 May 2004)

A security analysis of a recently proposed secure communication scheme based on the phase synchronization of chaotic systems is presented. It is shown that the system parameters directly determine the cipher text waveform, hence it can be readily broken by system parameter estimation from the cipher text signal. © *2004 American Institute of Physics.* [DOI: 10.1063/1.1688092]

Most secure chaotic communication systems are based on complete synchronization, whereas a new cryptosystem has been proposed based on phase synchronization. This scheme hides binary messages in the instantaneous phase of the drive subsystem used as the transmitting signal to drive the response subsystem. Although it is claimed to be secure against some traditional attacks in the chaotic cryptosystems literature, including the parameter estimation attack, we show that it is breakable by this attack. As a conclusion, the system is not secure and should not be used for communications where security is a strict requirement.

I. INTRODUCTION

The possibility of synchronization of two coupled chaotic systems was first shown by Pecora and Carroll.[1–3] The importance of this discovery was quickly appreciated,[4] and soon this topic aroused great interest as a potential means for communications.[5–10] In recent years, a great effort has been devoted to extend the chaotic communication applications to the field of secure communications. Accordingly, a great number of cryptosystems based on chaos have been proposed;[11–16] some of them fundamentally flawed by a lack of robustness and security.[17–28] All of them were based on complete synchronization of chaotic systems (CS). In Ref. 29, a new secure communication scheme based on the phase synchronization (PS) of a chaotic system is proposed.

PS of coupled chaotic oscillators with weak and strong coupling has been investigated extensively.[30–34] In PS, as opposed to CS, only the phases of the subsystems are locked and there is little correlation in signal amplitudes. In general, if the phase difference of two chaotic oscillators is bounded, the oscillators can be considered as phase synchronized.[31]

In this new scheme the drive and the response subsystems are strongly coupled, using the phase information as the transmitted cipher text. The plain text binary message b is hidden in the instantaneous phase of the drive subsystem. At the response subsystem, the phase difference is detected and its strong fluctuation above or below zero allows the plain text recovering at certain coupling strength.

The secure communication process is illustrated by means of an example based on coupled Rössler chaotic oscillators. In the example, the drive subsystem is formed by two weak coupled oscillators. The plain text is used to modulate the same parameter in both oscillators 1 and 2. The equations of the drive subsystem are

$$\begin{aligned}\dot{x}_{1,2} &= -(\omega+\Delta\omega)y_{1,2}-z_{1,2}+\varepsilon(x_{2,1}-x_{1,2}),\\ \dot{y}_{1,2} &= (\omega+\Delta\omega)x_{1,2}+\alpha y_{1,2},\\ \dot{z}_{1,2} &= 0.2+z_{1,2}(x_{1,2}-10).\end{aligned} \tag{1}$$

The response subsystem is governed by

$$\begin{aligned}\dot{x}_3 &= -\omega' y_3 - z_3 + \eta((x_3^2+y_3^2)^{1/2}\cos\phi_m - x_3),\\ \dot{y}_3 &= \omega' x_3 + \alpha' y_3,\\ \dot{z}_3 &= 0.2+z_3(x_3-10).\end{aligned} \tag{2}$$

In the example, the parameter values are: $\omega=\omega'=1$, $\varepsilon=5\times10^{-3}$, $\eta=5.3$, and $\alpha=\alpha'=0.15$.

The parameter ω corresponds to the natural frequency of the Rössler oscillator drive subsystems 1 and 2. The parameter ω' corresponds to the natural frequency of the Rössler oscillator driven subsystem 3, ε corresponds to the weak coupling factor between the oscillators 1 and 2, and η corresponds to the strong coupling factor in the driven oscillator 3.

The parameter mismatch $\Delta\omega$ is modulated by the plain text, being $\Delta\omega=0.01$ if the bit to be transmitted is "1" and $\Delta\omega=-0.01$ if the bit to be transmitted is "0."

The cipher text consists of the phase of the mean field of the two drive oscillators:

$$\phi_m = \arctan\frac{x_1+x_2}{y_1+y_2}. \tag{3}$$

At the receiving end the phase of the response subsystem is

$$\phi_3 = \arctan\frac{x_3}{y_3}.$$

[a]Electronic mail: gonzalo@iec.csic.es

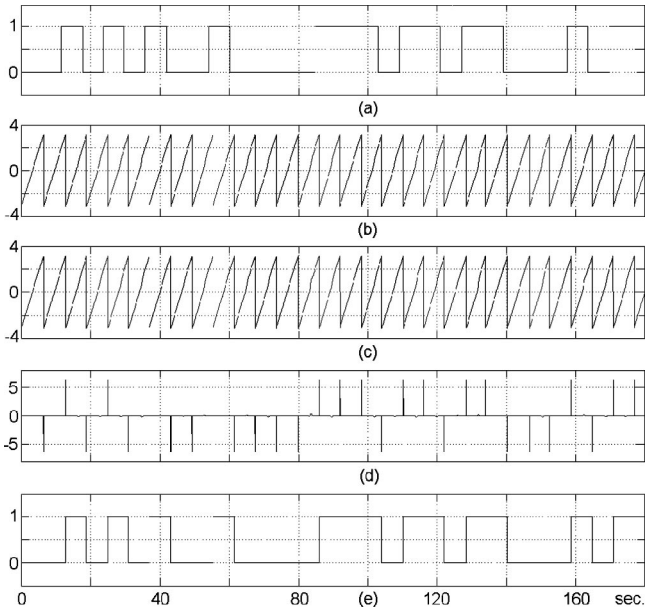

FIG. 1. Plain text recovery with the authorized receiver. Time histories of: (a) plain text b; (b) cipher text ϕ_m^*; (c) reconstructed phase signal of the response subsystem ϕ_3^*; (e) difference between the cipher text and the reconstructed signal $\phi_m^* - \phi_3^*$; (f) reconstructed plain text b'.

The detection of ''1'' or ''0'' in the response subsystem is related to different time delays between the drive and the response phases.

As the phase is a signal that has an unbounded amplitude, it cannot be transmitted through physical channels. The authors overcome this problem by coding the signal from π to $-\pi$, which corresponds to the Poincaré surface of the attractor at $y_{1,2}=0$. As a consequence, the transmitted cipher text, marked as ϕ_m^*, is a sawtooth-like signal with a frequency equal to the observed revolution frequency of the drive Rössler oscillators Ω. The phase at the receiving end is also coded from π to $-\pi$ as ϕ_3^*.

The plain text is retrieved by calculating the difference between the cipher text and the reconstructed signal, $\phi_m^* - \phi_3^*$. The difference signal consist of positive and negative peaks that correspond to the ones and zeros of the plain text.

The example of Ref. 29 is illustrated in Fig. 1. It was simulated with a four order Runge–Kutta integration algorithm in MATLAB 6, with a step size of 0.001. In order to recover the plain text with the exact waveform, allowing for a small time delay, a Smith-trigger was included as a reconstruction filter, with switch on point at 4 and switch off point at -4.

Given that in the example of Ref. 29 there is no indication about the parameter initial values, our simulation is implemented with the following initial values: $(x_1^{(0)},x_2^{(0)},x_3^{(0)},y_1^{(0)},y_2^{(0)},y_3^{(0)},z_1^{(0)},z_2^{(0)},z_3^{(0)}) = (-5,-3,-1,0,0,0,0,0,0)$.

The authors seem to base the security of its secure communication system on the properties of the phase synchronization. They claim that it cannot be broken by some traditional attacks used against secure chaotic systems with complete synchronization, but no general analysis of security is included.

Although the authors point out that the system parameters play the role of secret key in transmission (Ref. 29, Sec. V), it is not clearly specified which parameters are considered as candidates to form part of the key, what the allowable value range of those parameters is, what the key space is (how many different keys exist in the system) and how they should be managed. None of these elements should be neglected when describing a secure communication system.

Most papers on chaotic secure communications are published in physics journals and conferences, but not within the cryptography community; this explains why up to date little or no critical analysis has been made about the design process of these cryptosystems nor to the way the results are presented. Quoting Bao:[35] ''The common annoying feature of the cryptosystems based on some mathematical models, e.g., those based on chaos systems, is that only the principle is given. They lack details, such as recommended key sizes and key generation steps, etc. Therefore it is not possible for others to implement the ciphers.''

The weaknesses of this system and the method to break it are discussed in the next section.

II. BREAKING THE SYSTEM

The main problem with this cryptosystem lies on the fact that the cipher text is an analog signal, whose waveform depends on the system parameter values. Likewise, the difference between the cipher text and the phase signal of a nonsynchronized receiver $\phi_m^* - \phi_3^*$, depends on these same parameters. The study of these signals provides the necessary information to recover a good estimation of the system parameter values and the correct plain text, as will be seen next.

When cryptanalyzing a cryptosystem, the general assumption made is that the cryptanalyst knows exactly the design and working of the cryptosystem under study, i.e., he knows everything about the cryptosystem except the secret key. This is an evident requirement in today's secure communications systems, usually referred to as Kerchoff's principle.[36] In our attack, total knowledge of the communications system design is assumed. It is assumed too that the key consists of the oscillator's parameters α and ω, as they are the only unknowns in the example of Ref. 29. The key and the chaotic region which constitutes the key space from which valid keys are to be chosen should have been thoroughly specified in Ref. 29.

In our attack, the search space of the parameter α, that governs the topology of the chaotic attractor, is restricted to the unique suitable value range for operation. This range is characterized by the phase coherent chaotic region of the Rössler oscillator. Within this range, its phase increases monotonically with time, showing a chaotic increase rate, that allows hiding the binary information.

The operation of the system with values of α greater than a critical value α_c should be avoided because the Rössler oscillator becomes a ''wild'' funnel chaotic attractor, in which the phase is ill-defined. The value of α_c depends on the Rössler oscillator natural frequency ω ($\alpha_c \approx 0.186$ for $\omega = 0.98$ and $\alpha_c \approx 0.195$ for $\omega = 1.02$).[34] In such a case, the

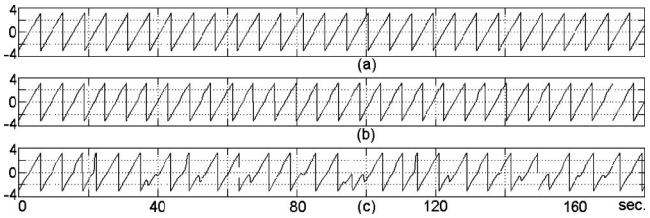

FIG. 2. Cipher text phase signal ϕ_m^* as function of α: (a) $\alpha=0.01$, the phase increases almost linearly; (b) $\alpha=0.15$, the phase increases monotonically with chaotic behavior; (c) $\alpha=0.25$, the phase increases and decreases irregularly.

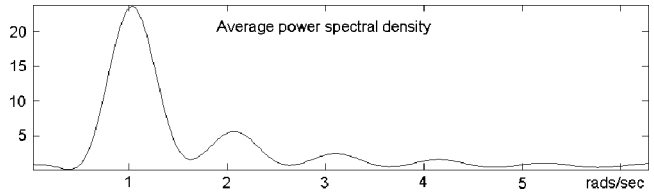

FIG. 3. Power spectral analysis of the cipher text signal. The highest peak corresponds to the frequency of Ω and lies at $\Omega\approx 1.1$.

phase definition of Eq. (3) employed by the authors is no longer applicable,[32] rendering it impossible the correct data retrieving by the authorized receiver.

Values of $\alpha<0.04$ should also be avoided because the oscillator exhibits a periodic motion with constant frequency, the waveform of the oscillator is uniform, and its phase increases linearly with time (Ref. 33, Sec. 3.1.1). Therefore, the instantaneous phase fluctuations, due to the binary information modulation, cannot be effectively hidden, and thus the information could be easily retrieved from the signal. Such kind of keys, that allow for immediate recovering of the plain text, are known in cryptography as *weak keys*.

In the example given in Ref. 29, with $\omega=1$, the coherent chaotic region is roughly characterized by the following values of α:

$$0.04\leqslant\alpha\leqslant 0.19. \tag{4}$$

The behavior of the attractor with respect to α is illustrated in Fig. 2, in which the time history of the cipher text signal ϕ_m^* for three values of α is shown. The first sample corresponds to $\alpha=0.01$, showing that the phase increases linearly. The second one corresponds to $\alpha=0.15$, showing that the phase increases monotonically with chaotic behavior. The last sample corresponds to $\alpha=0.25$, showing that the phase increases and decreases irregularly.

The sensitivity to the parameter values is so low that the original plain text can be recovered from the cipher text using an intruder receiver system with parameter values considerably different from the ones used by the transmitter. In Ref. 29 (Fig. 7), it is shown that for $\{\alpha',\omega'\}=\{0.15,1.00\}$ the allowable parameter mismatch of α' is $+0.022$, -0.028; and the allowable parameter mismatch of ω' is $+0.009,-0.004$.

We have found experimentally that for values of $\alpha\in[0,0.19]$ the plain text b' can be recovered even when α' has an absolute error of ± 0.02, what is in accordance with Ref. 29, Fig. 7. As a consequence, it is sufficient to try five values of α', to cover the whole coherent region. The best set of values is: $\alpha'=\{0.01,0.05,0.09,0.13,0.17\}$. In cryptography, when breaking a cryptosystem trying all possible keys (what it is called *brute force analysis*) the weak keys are routinely checked. Hence, we have also included in the search space the value $\alpha'=0.01$, that corresponds to the periodic motion region.

In Fig. 3 the power spectral analysis of the cipher text signal is shown. As is well known, the frequency of the Rössler oscillator is totally evident. The spectrum's highest peak appears at $\Omega\simeq 1.03$, close to the parameter value of the drive subsystem $\omega=1$. Thus, by simply examining the cipher text, the second key element ω' is guessed with reasonable accuracy.

Note that the original motivation for using chaotic modulation to implement secure communications is that chaotic signals exhibit a noise-like, continuous, random and broad spectrum, that may appear like a fortuitous channel perturbation, helping for the concealment of valuable information and preventing to attract the attention of a casual observer. In contrast, the proposed system shows a spectrum with a very specific periodic pattern and a definite waveform that will attract an eavesdropper's attention.

Let ω' be the approximate value of ω. Once it is measured we can use it to recover the plain text in the following way.

First, we introduce the estimated value of ω' into an intruder receiver with $\eta=0$, that is, without coupling, so the intruder receiver oscillator will be running freely. To check whether the estimation of ω' is good, we look at the output of the phase comparator $\phi_m^*-\phi_3^*$ as well as at the cipher text signal ϕ_m^*, and at the phase signal of the receiver ϕ_3^*.

When the frequencies of the transmitter and intruder receiver are slightly different, then $\phi_m^*-\phi_3^*$ will look like a train of pulses of increasing width summed with a direct current of increasing level, being the final width and direct current increasing level rate proportional to the difference of frequencies $\omega'-\omega$. Also, the mismatch of the periods of the phase signals ϕ_m^* and ϕ_3^* is perceptible. With this information we can adjust the value of ω' in a few steps, until the width of the pulses tends to zero. Then, the period mismatch of the phase signals ϕ_m^* and ϕ_3^* is unnoticeable and its direct current level equals zero.

The procedure is illustrated in Fig. 4. We begin with $\omega'=1.03$, the value estimated from the spectrum, and we see that the correct value of ω' must be slightly lower, thus we try $\omega'=1.015$ and we see that we are near the exact value but still a little bit higher. Next, we try $\omega'=1.005$, and we see that the frequency match is quite good. This last value of ω' is retained as the definite one.

Next, we set $\eta=5.3$ at the intruder receiver and look at the retrieved data b' for the previously obtained ω' and for each of the five possible values of α'. In Fig. 5 the retrieved binary data b' obtained with $\omega'=1.005$ and $\alpha'=\{0.01,0.05,0.09,0.13,0.17\}$ are presented. It can be seen that for $\alpha'=\{0.01,0.05,0.09,0.13\}$ only zero value data are obtained. For $\alpha'=0.17$, some output data are present, thus we assume that the value of $\alpha'=0.17$ can be retained as the

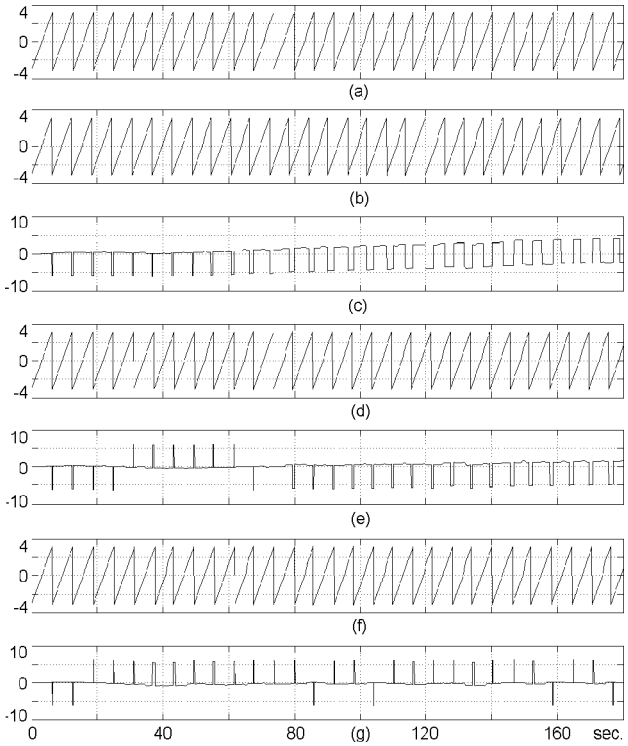

FIG. 4. Determination of the best value of ω': (a) cipher text signal with frequency $\omega=1.00$; (b) phase signal of the free running intruder receiver ϕ_3^* for $\omega'=1.03$; (c) output of the phase comparator $\phi_m^*-\phi_3^*$ for $\omega'=1.03$; (d) phase signal of the free running intruder receiver ϕ_3^* for $\omega'=1.015$; (e) output of the phase comparator $\phi_m^*-\phi_3^*$ for $\omega'=1.015$; (f) phase signal of the free running intruder receiver ϕ_3^* for $\omega'=1.005$; (g) output of the phase comparator $\phi_m^*-\phi_3^*$ for $\omega'=1.005$.

appropriate one to retrieve the plain text b' and that the data obtained with it consists of the correct recovered plain text, as can be verified from the figure.

Although the estimated pair of values $\{\omega',\alpha'\}=\{1.005,0.17\}$ are not exactly the right ones, the plain text is correctly recovered as a consequence of the system's low sensitivity to parameters. Therefore, the claim by the authors

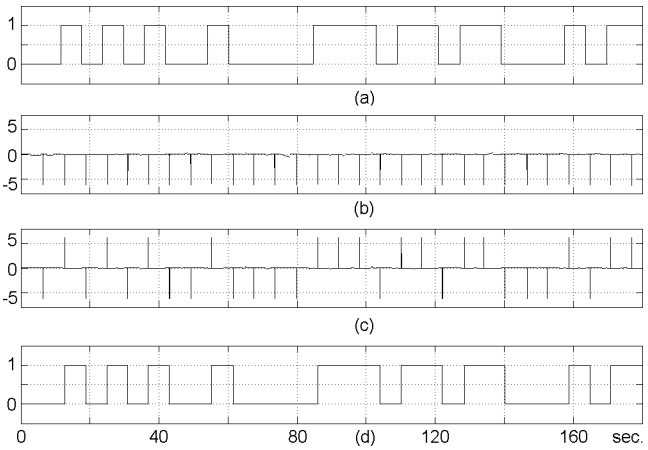

FIG. 5. Determination of the best value of α', with $\omega'=1.005$: (a) original plain text, b; (b) output of the phase comparator $\phi_m^*-\phi_3^*$ for $\alpha'=\{0.01,0.05,0.09,0.13\}$, which is the same in three cases; (c) output of the phase comparator $\phi_m^*-\phi_3^*$ for $\alpha'=0.17$; (d) recovered plain text b' for $\alpha'=0.17$.

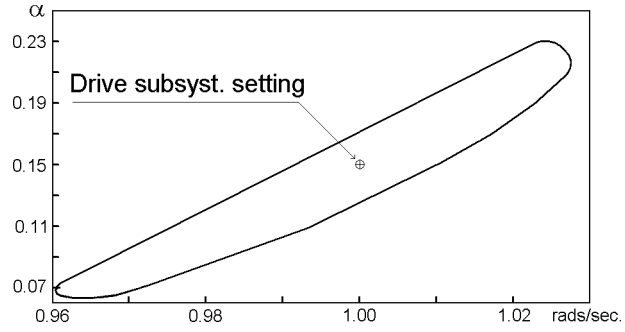

FIG. 6. Range of ω' and α' values that achieve correct plain text recovery of a cipher text generated with $\{\omega,\alpha\}=\{1.00,0.15\}$.

of Ref. 29 that the scheme is difficult to be broken by traditional attacks, as the parameter identification method, is unfounded.

Moreover, we have observed that many other combinations of parameter values allow for the recovery of the correct plain text as well. In Fig. 6 it is shown, after many simulations, the region of $\{\omega',\alpha'\}$ values in which correct plain text recovery of a cipher text generated with a drive subsystem with $\{\omega,\alpha\}=\{1.00,0.15\}$ is achieved.

III. CONCLUSION

The proposed cryptosystem is rather weak, since it can be broken by measuring the power spectrum of the cipher text signal and trying a small set of parameter values. There is no detailed description about what the key is, nor what the key space is, a fundamental aspect in every secure communication system. The lack of security discourages the use of this algorithm for secure applications.

ACKNOWLEDGMENT

This work is supported by Ministerio de Ciencia y Tecnología of Spain, research Grant No. TIC2001-0586.

[1] L. M. Pecora and T. L. Carroll, "Synchronization in chaotic systems," Phys. Rev. Lett. **64**, 821–824 (1990).
[2] L. M. Pecora and T. L. Carroll, "Driving systems with chaotic signals," Phys. Rev. A **44**, 2374–2383 (1991).
[3] T. L. Carroll and L. M. Pecora, "Synchronizating chaotic circuits," IEEE Trans. Circuits Syst. **38**, 453–456 (1991).
[4] R. He and P. G. Vaidya, "Analysis and synthesis of synchronous periodic and chaotic systems," Phys. Rev. A **46**, 7387–7392 (1992).
[5] G. Kolumbán, M. P. Kennedy, and L. O. Chua, "The role of synchronization in digital communication using chaos. Part I. Fundamentals of digital communications," IEEE Trans. Circuits Syst., I: Fundam. Theory Appl. **44**, 927–936 (1997).
[6] G. Kolumbán, M. P. Kennedy, and L. O. Chua, "The role of synchronization in digital communication using chaos. Part II. Chaotic modulation and chaotic synchronization," IEEE Trans. Circuits Syst., I: Fundam. Theory Appl. **45**, 1129–1140 (1998).
[7] G. Kolumbán and M. P. Kennedy, "The role of synchronization in digital communication using chaos. Part III. Performance bounds," IEEE Trans. Circuits Syst., I: Fundam. Theory Appl. **47**, 1673–1683 (2000).
[8] H. Dedieu, M. P. Kennedy, and M. Hasler, "Chaos shift keying: Modulation and demodulation of chaotic carrier using self-synchronizing Chuass circuits," IEEE Trans. Circuits Syst., II: Analog Digital Signal Process. **40**, 634–642 (1993).
[9] L. Kocarev and U. Parlitz, "General approach for chaotic synchronization with applications to communication," Phys. Rev. Lett. **74**, 5028–5031 (1995).

[10] C. K. Tse and F. C. M. Lau, *Chaos-Based Digital Communication Systems: Operating Principles, Analysis Methods, and Performance Evaluation* (Springer Verlag, Berlin, 2003).
[11] K. M. Cuomo and A. V. Oppenheim, ''Circuit implementation of synchronized chaos with applications to communications,'' Phys. Rev. Lett. **71**, 65–68 (1993).
[12] K. M. Cuomo, A. V. Oppenheim, and H. Strogatz, ''Synchronization of Lorenz-based chaotic circuits with applications to communications,'' IEEE Trans. Circuits Syst., II: Analog Digital Signal Process. **40**, 626–633 (1993).
[13] C. W. Wu and L. O. Chua, ''A simple way to synchronize chaotic systems with applications to secure communication systems,'' Int. J. Bifurcation Chaos Appl. Sci. Eng. **3**, 1619–1627 (1993).
[14] C. W. Wu and L. O. Chua, ''Secure communication via chaotic synchronization II: Noise reduction by cascading two identical receivers,'' Int. J. Bifurcation Chaos Appl. Sci. Eng. **3**, 1319–1325 (1993).
[15] T. Yang, ''A survey of chaotic secure communication systems,'' Int. J. Comp. Cognition **2**, 81–130 (2004).
[16] G. Álvarez, F. Montoya, M. Romera, and G. Pastor, ''Chaotic cryptosystems,'' in *33rd Annual 1999 International Carnahan Conference on Security Technology*, edited by L. D. Sanson (IEEE, New York, 1999), pp. 332–338.
[17] K. M. Short, ''Steps toward unmasking secure communications,'' Int. J. Bifurcation Chaos Appl. Sci. Eng. **4**, 959–977 (1994).
[18] T. Beth, D. E. Lazic, and A. Mathias, ''Cryptanalysis of cryptosystems based on remote chaos replication,'' in *Advances in Cryptology—CRYPTO '94*, Vol. 839 in *Lecture Notes in Computer Science*, edited by Y. G. Desmedt (Springer-Verlag, Berlin, 1994), pp. 318–331.
[19] G. Pérez and H. A. Cerdeira, ''Extracting messages masked by chaos,'' Phys. Rev. Lett. **74**, 1970–1973 (1995).
[20] K. M. Short, ''Unmasking a modulated chaotic communications scheme,'' Int. J. Bifurcation Chaos Appl. Sci. Eng. **6**, 367–375 (1996).
[21] H. Zhou and X. Ling, ''Problems with the chaotic inverse system encryption approach,'' IEEE Trans. Circuits Syst., I: Fundam. Theory Appl. **44**, 268–271 (1997).
[22] T. Yang, L. B. Yang, and C. M. Yang, ''Breaking chaotic switching using generalized synchronization: Examples,'' IEEE Trans. Circuits Syst., I: Fundam. Theory Appl. **45**, 1062–1067 (1998).
[23] T. Yang, L. B. Yang, and C. M. Yang, ''Breaking chaotic secure communications using a spectogram,'' Phys. Lett. A **247**, 105–111 (1998).
[24] T. Yang, L. B. Yang, and C. M. Yang, ''Cryptanalyzing chaotic secure communications using return maps,'' Phys. Lett. A **245**, 495–510 (1998).
[25] G. Álvarez, F. Montoya, M. Romera, and G. Pastor, ''Cryptanalysis of a chaotic encryption system,'' Phys. Lett. A **276**, 191–196 (2000).
[26] G. Álvarez, F. Montoya, M. Romera, and G. Pastor, ''Cryptanalysis of a chaotic secure communication system,'' Phys. Lett. A **306**, 200–205 (2003).
[27] G. Álvarez, F. Montoya, M. Romera, and G. Pastor, ''Cryptanalysis of an ergodic chaotic cipher,'' Phys. Lett. A **311**, 172–179 (2003).
[28] S. Li, X. Mou, Y. Cai, Z. Ji, and J. Zhang, ''On the security of a chaotic encryption scheme: Problems with computerized chaos in finite computing precision,'' Comput. Phys. Commun. **153**, 52–58 (2003).
[29] J. Y. Chen, K. W. Wong, L. M. Cheng, and J. W. Shuai, ''A secure communication scheme based on the phase synchronization of chaotic systems,'' Chaos **13**, 508–514 (2003).
[30] M. G. Rosenblum, A. S. Pikovsky, and J. Kurths, ''Phase synchronization of chaotic oscillators,'' Phys. Rev. Lett. **76**, 1804–1807 (1996).
[31] U. Parlitz, L. Junge, W. Lauterborn, and L. Kocarev, ''Experimental observation of phase synchronization,'' Phys. Rev. E **54**, 2115–2117 (1996).
[32] M. G. Rosenblum, A. S. Pikovsky, J. Kurths, G. V. Osipov, I. Z. Kiss, and J. L. Hudson, ''Locking-based frequency measurement and synchronization of chaotic oscillators with complex dynamics,'' Phys. Rev. Lett. **89**, 264102 (2002).
[33] S. Boccaletti, J. Kurths, G. Osipov, D. L. Valladares, and C. S. Zhou, ''The synchronization of chaotic systems,'' Phys. Rep. **366**, 1–101 (2002).
[34] G. V. Osipov, B. Hu, C. Zhou, M. V. Ivanchenko, and J. Kurths, ''Three types of transitions to phase synchronization in coupled chaotic oscillators,'' Phys. Rev. Lett. **91**, 024101 (2003).
[35] F. Bao, ''Cryptanalysis of a new cellular automata cryptosystem,'' ACISP, pp. 416–427 (2003).
[36] D. R. Stinson, *Cryptography: Theory and Practice* (CRC Press, Boca Raton, 1995).