Multiplexed encryption using chaotic systems with multiple stochastic-delayed feedbacks

Damien Rontani, Marc Sciamanna, A. Locquet, D S Citrin

Multiplexed encryption using chaotic systems with multiple stochastic-delayed feedbacks

D. Rontani,[1,2,3] M. Sciamanna,[2,1] A. Locquet,[1,3] and D. S. Citrin[1,3]
[1]*UMI 2958 Georgia Tech–CNRS, Georgia Tech Lorraine, 2-3 Rue Marconi, 57070 Metz, France*
[2]*Supélec–LMOPS EA-4423, 2 Rue Edouard Belin, 57070 Metz, France*
[3]*School of Electrical and Computer Engineering, Georgia Institute of Technology, Atlanta, Georgia 30332-0250, USA*
(Received 29 April 2009; revised manuscript received 21 September 2009; published 21 December 2009)

We propose an efficient and fast bit-multiplexed encryption scheme exploiting hyperchaotic regimes of a single nonlinear oscillator with multiple time-delay feedback loops. Each data stream is encrypted by digitally modulating the values of the various time delays and decrypted using chaos synchronization and cross-correlation measurements. We have numerically applied our approach to an optoelectronic chaotic oscillator based on standard semiconductor lasers subjected to multiple feedbacks and have demonstrated successful data transmission and recovery between multiple users at several Gbits/s on a single communication channel.

DOI: 10.1103/PhysRevE.80.066209 PACS number(s): 05.45.Vx, 05.45.Xt, 42.65.Sf

The peculiar properties of chaotic oscillators have contributed to the development of innovative approaches to secure communications where security is ensured at the physical level [1–4]. Chaotic oscillators generate a deterministic noiselike signal, called the chaotic carrier, that can be used to convey and conceal information between emitter Alice and authorized receiver Bob. Chaos synchronization, whereby the chaotic dynamics of the receiver locks to the chaotic dynamics of the emitter [5], is then generally used for message retrieval. These chaos-based-communication schemes and their synchronization properties have been extensively studied in electrical [6,7] and optical systems [8–15].

Suppose, however, each of a set of transmitters, Alice$_i$ ($i=1,\ldots,N$), wishes to securely send a message to a respective receiver, Bob$_i$, on the same shared physical communication channel. Indeed, it is necessary for the Alices to simultaneously transmit different data streams and for their respective Bobs to decrypt them independently and to minimize the inevitable interferences produced by the other users. Wavelength-division multiplexing (WDM) and time-division multiplexing (TDM) are typical approaches to solve the problem. WDM has been already adapted for chaotic optical systems [16–18]; however, it requires the various users to divide the channel into dedicated spectrum slices. More spectrally efficient methods to multiplex chaotic carriers and information-bearing messages have been proposed but require either as many chaotic oscillators as users to encrypt and decrypt with a low level of complexity [19–23] or a single oscillator is used but requires a complex structure for decryption [24].

In this paper, we show how time-delay systems can be used favorably to overcome simultaneously these two major limitations in chaos multiplexing. We use a *single* chaotic oscillator with N time-delay feedback loops, each of the time delays being digitally modulated by a specific user. This approach, which is neither the overlay of TDM nor of WDM on top of a conventional chaotic system, uses a single chaotic oscillator that ensures the simultaneous encryption of N messages in a single wide-spectrum chaotic carrier. This is therefore beneficial to achieve higher spectral efficiency on the communication-channel bandwidth in comparison with WDM. Extraction of the various messages is realized with a low-complexity decryption strategy based on finite-time cross-correlation measurements. Additionally, the stochastic modulation of the time delays at the rate of the messages participates in the dynamical evolution of the chaotic oscillator and contributes to enhancing the security of transmission. We numerically apply our multiplexing/demultiplexing technique to an optoelectronic chaos generator based on a well-tested and reliable physical model and demonstrate theoretically multi-Gbit/s transmission per user for four users.

The proposed multiplexing scheme is depicted in Fig. 1. It is comprised of emitter E coupled via a communication channel to receiver R carrying signal $s(t)$. The emitter E is a time-delay nonlinear oscillator fed back with $s(t)$ which is the sum of the outputs of N time-delayed feedback loops. The receiver R is an open-loop copy of the emitter E with the same nonlinear oscillator and with N decryption branches using the same elements as those of E's feedback loops. Assuming zero time of flight between E and R, the dynamical behaviors of these two systems are described by

$$\dot{\mathbf{x}}_E = f(\mathbf{x}_E, s), \quad \dot{\mathbf{x}}_R = f(\mathbf{x}_R, s), \tag{1}$$

where $\mathbf{x}_E, \mathbf{x}_R \in \mathbb{R}^n$ are the state vectors of E and R, respectively, and $s \in \mathbb{R}$. This architecture, where a single signal s drives the dynamics of E and R in the same way, corresponds to an active-passive-decomposition (APD) configuration [25]. The encryption of each information-bearing message m_i is realized by modulating the ith time-delay value τ_i at the rhythm of the ith message m_i. Each message m_i is composed of M_i discrete symbols $\{c_1^{(i)},\ldots,c_{M_i}^{(i)}\}$ which code the time-delay values taken by τ_i in time interval $\Delta_i=[\tau_{i0}-\frac{\Delta\tau_i}{2},\tau_{i0}+\frac{\Delta\tau_i}{2}]$ called the encryption slot. Figure 2 illustrates the generation of symbols by the ith user. Alice$_i$ sequentially generates various time delays $\tau_{i|\Omega_k}$ on consecutive symbol time slots $\Omega_k=[kT_s,(k+1)T_s]$ where k indexes the time slot corresponding to the kth symbol and T_s is the symbol duration. This results in a digitally modulated time delay $\tau_i=\Sigma_k\tau_{i|\Omega_k}\{H(t-kT_s)-H[t-(k+1)T_s]\}$, where H is the Heaviside function. Encryption on the time-delay value was originally proposed for a single binary message in Ref. [26], but our encryption approach differs as it allows for the encryption of multiple M-ary messages.

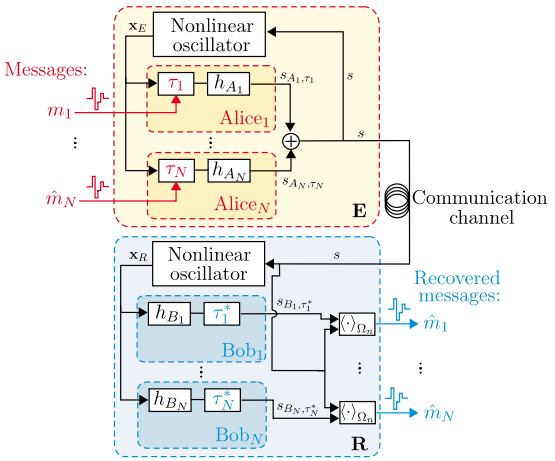

FIG. 1. (Color online) Schematic configuration for multiplexed encryption based on APD and using a nonlinear oscillator with a delayed feedback loop for each of the N users.

In each feedback loop, the time delay is then embedded in the chaotic wave forms $s_{A_i,\tau_i}=h_{A_i}(\mathbf{x}_{E,\tau_i})$ with $\mathbf{x}_{E,\tau_i}=\mathbf{x}_E(t-\tau_i)$ and h_{A_i} a nonlinear function. Finally, the N users combine their wave forms in a single chaotic signal (cf. Fig. 1) $s(t)=\Sigma_{i=1}^{N}s_{A_i,\tau_i}$.

Decryption relies on the independent retrieval of the symbols $c_\mu^{(i)}$ $(\mu=1,\ldots,M_i,\ i=1,\ldots,N)$ used by the Alices to represent the time delays for all symbol time slots Ω_k. It is assumed that each receiver Bob$_i$ only knows Alice$_i$'s key, which is constituted by the set (T_s,h_{A_i},f) and has R completely synchronized with E. Consequently, he can use this information to generate a *candidate* chaotic wave form $s_{B_i,\tau^*_{i|\Omega_k}}=h_{B_i}(\mathbf{x}_{R,\tau^*_{i|\Omega_k}})=h_{A_i}(\mathbf{x}_{E,\tau^*_{i|\Omega_k}})$ with an arbitrary value for the delay $\tau^*_{i|\Omega_k}$ belonging to Δ_i. This requires Bob$_i$ to store the history of receiver R during $\tau_{m,i}=\max\Delta_i$ the maximum possible value of τ_i in the encryption slot. It is clear that Bob$_i$'s wave form $s_{B_i,\tau^*_{i|\Omega_k}}$ is identical to Alice$_i$'s wave form $s_{A_i,\tau_{i|\Omega_k}}$ on Ω_k if and only if $\tau^*_{i|\Omega_k}=\tau_{i|\Omega_k}$. This property will be used for the retrieval of $\tau_{i|\Omega_k}$. To help us explain the decryption process, we define a finite-time cross-correlation function between two arbitrary signals φ_i and φ_j on a symbol time slot Ω_k, $\langle\varphi_i,\varphi_j\rangle_{\Omega_k}=\int_{kT_s}^{(k+1)T_s}\varphi_i(u)\varphi_j(u)du$. First, Bob$_i$ starts by computing the cross-correlation $\langle s,s_{B_i,\tau^*_{i|\Omega_k}}\rangle_{\Omega_k}$ between the transmitted signal s, which is the sum of the N Alices' wave forms $s_{A_i,\tau_{i|\Omega_k}}$, and the wave form he generates $s_{B_i,\tau^*_{i|\Omega_k}}$. Then, the recovery of Alice$_i$'s encoded symbol $\tau_{i|\Omega_k}$ requires three necessary conditions: (i) the cross-correlation measurement must present a dominant local maximum (resonance) at $\tau^*_{i|\Omega_k}=\tau_{i|\Omega_k}$, (ii) this resonance must correspond to a time delay from a unique Alice$_i$ targeted at Bob$_i$ only, and (iii) two symbols belonging to the same message in a given encryption slot must be separable by a cross-correlation measurement. When the three decryption conditions are met, each user Bob$_i$ can estimate Alice$_i$'s symbol $\tau_{i|\Omega_k}$ by locating the delay value $\hat{\tau}_{i|\Omega_k}$ that maximizes the cross-correlation measurement,

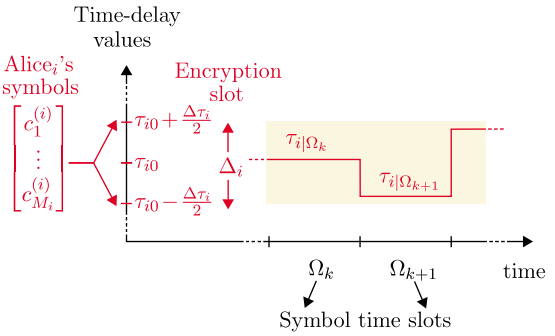

FIG. 2. (Color online) Graphical representation of the time-delay encryption performed by Alice$_i$ in her specific encryption slot Δ_i. She is encrypting two consecutive symbols through the time delays $\tau_{i|\Omega_k}$ and $\tau_{i|\Omega_{k+1}}$.

$$\hat{\tau}_{i|\Omega_k}=\arg\max_{\tau^*_{i|\Omega_k}\in\Delta_i}\langle s,s_{B_i,\tau^*_{i|\Omega_k}}\rangle_{\Omega_k}. \tag{2}$$

The messages encrypted by the other Alices are then decrypted using exactly the same procedure. Interestingly, the complexity of decryption for Bob$_i$ is independent of the number of users N.

The fulfillment of conditions (i)–(iii) is realized by imposing specific design constraints on our communication scheme. They are analyzed below. Condition (i) is satisfied if $\langle s,s_{B_i,\tau^*_{i|\Omega_k}}\rangle_{\Omega_k}$ has a unique dominant maximum for Bob$_i$. This cross-correlation reveals two contributions:

$$\langle s,s_{B_i,\tau^*_{i|\Omega_k}}\rangle_{\Omega_k}=\langle s_{A_i,\tau_{i|\Omega_k}},s_{B_i,\tau^*_{i|\Omega_k}}\rangle_{\Omega_k}+\sum_{j=1,j\neq i}^{N}\langle s_{A_j,\tau_{j|\Omega_k}},s_{B_i,\tau^*_{i|\Omega_k}}\rangle_{\Omega_k}. \tag{3}$$

The first term on the right-hand side of Eq. (3) is responsible for the local resonance at $\tau^*_{i|\Omega_k}=\tau_{i|\Omega_k}$ and the second term produces an essentially constant *background* value independent of $\tau^*_{i|\Omega_k}$. The detection of the dominant resonance at $\tau_{i|\Omega_k}$ relies on the choice of nonlinear functions h_{A_i} that allows its extraction from the cross-correlation background. This background can considerably disturb the decryption process of correlation-based communication schemes if not properly minimized. This usually imposes stringent decorrelation requirements between the different chaotic carriers [22]. In our case, more flexibility is permitted; with a proper choice for the nonlinear functions h_{A_i}, the resonance is detectable even with a significant correlation background. Condition (i) also imposes a lower bound for the symbol duration T_s. Indeed, cross-correlation measurements are reliable only if the oscillator exhibits sufficient dynamical diversity during T_s. This provides a lower bound for T_s equal to a few times the decorrelation time of $s(t)$. Condition (ii) can be met if all distinct pairs of encryption slots $(\Delta_i,\Delta_j)_{i\neq j}$ are disjoint and if their separation exceeds a global decorrelation time defined as $\delta_c=\max_i\delta_{ci}$ where δ_{ci} is the natural decorrelation time of the chaotic carrier s_{A_i,τ_i}. Condition (iii) is satisfied when the density of symbols per encryption slot does not exceed the resolution limit of cross-correlation measurements.

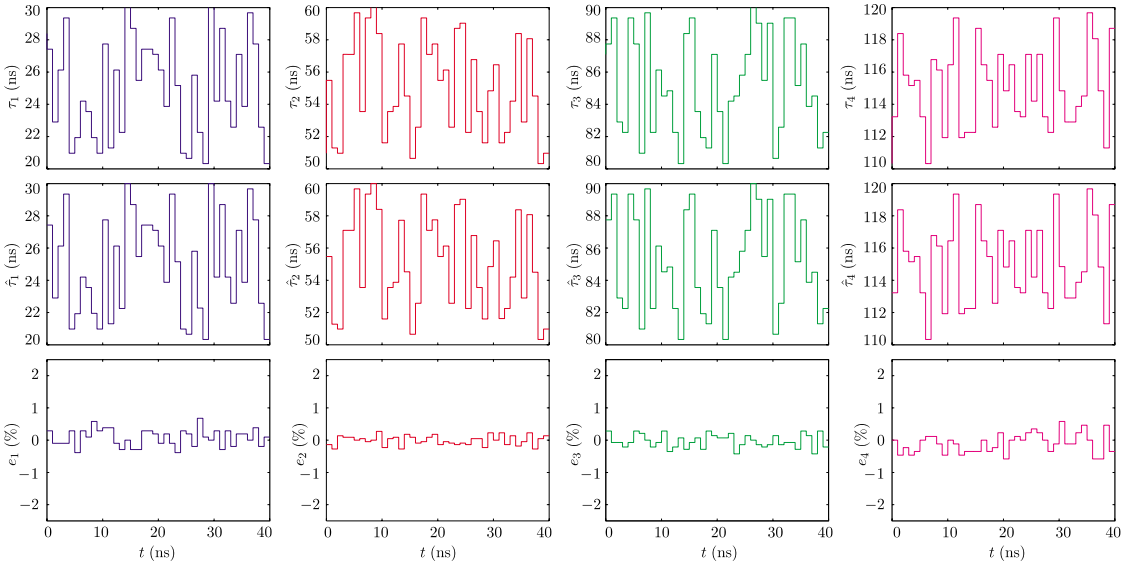

FIG. 3. (Color online) Simultaneous decryption of four messages composed of $M_i=32$ $(i=1,\ldots,4)$ symbols at 1 Giga symbols/s per user. The equivalent bit rate is 5 Gbits/s per user. The first line gives input messages τ_i, the second line the recovery messages $\hat{\tau}_i$, and the third line relative error e_i on each decrypted symbol in percentage. The equivalent aggregate bit rate is 20 Gbits/s.

Following this theoretical framework, we apply numerically our approach to a transmission chain composed of two coupled optoelectronic oscillators subjected to four delayed feedback loops to transmit $N=4$ independent messages. The oscillators correspond to optoelectronic intensity chaos generators based on Mach-Zehnder intensity modulators in their nonlinear regimes and subjected to time-delay feedback on the electrodes that drive the modulating effects. The feedback is implemented by adding to the bias voltage another voltage which is a function of the optical intensity measured by a photodiode at the output of the Mach-Zehnder. The coupled oscillators are known to be modeled by the set of integro-differential delay equations [27]

$$T\dot{\mathbf{x}}_E + \mathbf{x}_E + \frac{1}{\theta}\int_{t_0}^{t} \mathbf{x}_E(u)du = \sum_{i=1}^{4} \beta_i \cos^2(\mathbf{x}_{E,\tau_i} + \phi_{0i}), \quad (4)$$

$$T\dot{\mathbf{x}}_R + \mathbf{x}_R + \frac{1}{\theta}\int_{t_0}^{t} \mathbf{x}_R(u)du = \sum_{i=1}^{4} \beta_i \cos^2(\mathbf{x}_{E,\tau_i} + \phi_{0i}), \quad (5)$$

where $\mathbf{x}_E$, $\mathbf{x}_R$ are the dimensionless driving voltages of E and R, respectively, T is the high cutoff response time, θ is the low cutoff response time, β_i is the normalized feedback strength of the ith Mach-Zehnder modulator, and ϕ_{0i} is its normalized offset phase. This system of equations can be rewritten in ordinary differential form if the variable change $\mathbf{y}_{E,R}=\frac{1}{T}\int_{t_0}^{t}\mathbf{x}_{E,R}(u)du$ is introduced, and thus the above theory can be applied. We have simulated the coupled systems using the following parameter values: $T=25$ ps, $\theta=10$ μs, $\Delta_i=[20i$ ns$,20i+10$ ns$]$, $\phi_{0i}=\frac{2\pi i}{4}$, and $\beta_i=30$ $(i=1,\ldots,4)$. This corresponds to a particular case of our general approach where $h_{A_i}(\mathbf{x}_{E,\tau_i})=\beta_i\cos^2(\mathbf{x}_{E,\tau_i}+\phi_{0i})$ and $s(t)=\Sigma_{i=1}^{4}\beta_i\cos^2(\mathbf{x}_{E,\tau_i}+\phi_{0i})$. Each user Alice$_i$ has a data source of $M_i=32$ symbols which correspond to 32 time delays belonging to the encryption slot Δ_i.

Figure 3 shows the numerical results with ideal transmission conditions: no noise and no distortion induced by the communication channel. The symbols are maintained constant during symbol time slots of a duration $T_s=1$ ns. This leads to 1 Giga symbols/s transmission per user and appears to be the lower bound of T_s when four users send their messages. This corresponds to an equivalent 5 Gbits/s transmission per user considering that each symbol requires 5 bits to be encoded. The first and the second rows in Fig. 3 represent the data randomly generated by each user Alice$_i$ and the data recovered by the corresponding receiver Bob$_i$, respectively. The third row displays, for each user, the relative errors $e_i=(\tau_i-\hat{\tau}_i)/\tau_i$ in symbols recovery, which are all on average smaller than 0.5%. The errors are due to uncertainties in the detection of the maximum cross-correlation in the short intervals Ω_k. They can be suppressed if the Bobs know *a priori* the sets of possible symbols used by the Alices as would be expected when digital symbols are used. This proves that near-perfect decryption is achieved for four digital messages and also that these can be encoded on a large number of symbols. Correct decryption at a given symbol rate $1/T_s$ is also dependent on the number of users N. It affects the amplitude of the background fluctuations present in the correlation $\langle s, s_{B_i,\tau^*_{i|\Omega_k}}\rangle$, thus, increasing the probability to infer an incorrect value of $\tau_{i|\Omega_k}$ from $\tau^*_{i|\Omega_k}$. This induces a decrease in the largest achievable bit rate when the number of users increases. As an illustration, maintaining identical parameters to those above, we achieve (results not shown) a maximum of six users, resulting in an equivalent aggregate bit rate of 30 Gbits/s. Additional simulations including realistic levels of additive noise in E and R demonstrate robustness of our communication scheme with an average decryption error below 1%.

The security in our approach benefits from the fast stochastic and independent oscillations of each time delay on which data is encoded. It is known that fixed time-delay

systems face security flaws when the values of the time delays are known. Despite their high dimensionality [28–31], an eavesdropper can attack these systems in a low-dimensional space corresponding to the actual state space dimension of the system and where the nonlinear function of the system is identifiable at a low computational cost then allowing an easy reconstruction of the emitter dynamics by analyzing the time series of the transmitted signal [32,33]. Consequently, it is necessary to conceal the time delays to maintain sufficient computational security. For this purpose, random commutation between two time delays [34] and stochastic evolution of the time delay over a continuous range of values [35] have been proposed. Our approach corresponds to a generalization of the two-delay case where M_i different symbol values are used for each delay. It has been shown that in the case of a single emitter using two symbols encoded on two delays ($N=1$, $M_1=2$) a commutation time T_s smaller than the smallest symbol value prevents an eavesdropper from sequentially cracking E using sections of the transmitted time series of length T_s where the delays are maintained constant [34]. Thus, to fulfill security requirements in our multiuser case, it is necessary for the symbol duration to satisfy $T_s \leq \min_{i,k} \tau_{i|\Omega_k}$. This gives an upper bound to the symbol duration for the time delays, when $s(t)$ is analyzed. Shifting correlation and mutual-information attacks have been carried out to test the security of the system. No meaningful information on the data streams transmitted by each Alice has been obtained, even when, as proposed in [34], the attacks are performed on the duration of a single bit, which we assume to be known. The number M_i of symbols used to encode Alice$_i$'s data source also plays a significant role in the security. Indeed, if a realistic data source is employed, it may present repetitive patterns. This is particularly true in the case of binary data streams. The consecutive repetition of the same bit during many periods T_s could help an eavesdropper getting information about the correspondence between the binary symbols ("0" and "1") and the time-delay values. In the case of $M_i=2$, the security is similar to the one described in [34] except that the commutations are not controlled by data sources facing a repetition problem on consecutive symbol time slots Ω_k. However, if instead of encoding a binary digit of information on two time-delay values, a block of $\log_2 M_i$ bits is encoded, we create a correspondence between M_i different blocks of bits and M_i different time delays. This is beneficial in many ways for our system. First, it can capture large repetitive structures of bits and encode them as single time-delay values. Second, it increases Alice$_i$'s bit rate by a factor $\log_2 M_i$. Finally, as M_i is growing and if T_s is small enough, it increases the number of values to commute between and, thus, the fast digital random commutations can be considered as acting close to a continuous-valued continuous-time stochastic process for which security with respect to correlation-based attacks has been demonstrated [35]. Finally, this suggests that the Alices should employ sets of symbols as large as possible to tend to a stochastic evolution of the delay. Nevertheless, the decryption method has a finite resolution, which intrinsically limits the density of symbols to be encoded per finite-size encryption slot [see condition (iii)], and the equivalent achievable bit rate. These conditions, relative to security, complement the design constraints (i)–(iii) in the realization of a secure multiplexed chaos-based communication scheme.

In this paper, we have demonstrated the ability of a cryptosystem to encrypt N different messages using a single nonlinear oscillator subjected to N time-delayed feedback loops and to decrypt these messages using a synchronization-based technique. Our method combines the stochasticity of the data sources and the hyperchaotic behavior of time-delay systems in an efficient and secure way. This contrasts with previous chaos multiplexing approaches where each data source required its own oscillator to ensure low-complexity decryption. The simulation of an optoelectronic oscillator demonstrates four-users-transmission at multiple Gbits/s. This offers perspectives both in terms of bit rate, spectral efficiency, and security enhancement for future multiuser chaos-based communications.

The authors acknowledge the support of Fondation Supélec and Région Lorraine. D.S.C. was supported in part by the National Science Foundation by ECCS Grants No. 0523923 and No. 0925713.

[1] S. Hayes, C. Grebogi, and E. Ott, Phys. Rev. Lett. **70**, 3031 (1993).
[2] G. D. VanWiggeren and R. Roy, Science **279**, 1198 (1998).
[3] A. Argyris, D. Syvridis, L. Larger, V. Annovazzi-Lodi, P. Colet, I. Fischer, J. Garcia-Ojalvo, C. R. Mirasso, L. Pesquera, and K. A. Shore, Nature (London) **437**, 343 (2005).
[4] V. S. Udaltsov, J.-P. Goedgebuer, L. Larger, and W. T. Rhodes, Phys. Rev. Lett. **86**, 1892 (2001).
[5] L. M. Pecora and T. L. Carroll, Phys. Rev. Lett. **64**, 821 (1990).
[6] K. M. Cuomo and A. V. Oppenheim, Phys. Rev. Lett. **71**, 65 (1993).
[7] U. Parlitz, L. O. Chua, L. Kocarev, K. S. Halle, and A. Shang, Int. J. Bifurcation Chaos **2**, 973 (1992).
[8] J.-M. Liu, H.-F. Chen, and S. Tang, IEEE J. Quantum Electron. **38**, 1184 (2002).
[9] S. Tang and J.-M. Liu, IEEE J. Quantum Electron. **39**, 708 (2003).
[10] C. R. Mirasso, P. Colet, and P. García-Fernández, IEEE Photon. Technol. Lett. **8**, 299 (1996).
[11] V. Ahlers, U. Parlitz, and W. Lauterborn, Phys. Rev. E **58**, 7208 (1998).
[12] T. Heil, I. Fischer, W. Elsässer, J. Mulet, and C. R. Mirasso, Phys. Rev. Lett. **86**, 795 (2001).
[13] E. Klein, N. Gross, M. Rosenbluh, W. Kinzel, L. Khaykovich, and I. Kanter, Phys. Rev. E **73**, 066214 (2006).
[14] J. Kestler, E. Kopelowitz, I. Kanter, and W. Kinzel, Phys. Rev. E **77**, 046209 (2008).
[15] Y. Aviad, I. Reidler, W. Kinzel, I. Kanter, and M. Rosenbluh, Phys. Rev. E **78**, 025204(R) (2008).

[16] A. Uchida, S. Kinugawa, T. Matsuura, and S. Yoshimori, Opt. Lett. **28**, 19 (2003).
[17] T. Matsuura, A. Uchida, and S. Yoshimori, Opt. Lett. **29**, 2731 (2004).
[18] J. Paul, S. Sivaprakasam, and K. A. Shore, J. Opt. Soc. Am. B **21**, 514 (2004).
[19] L. S. Tsimring and M. M. Sushchik, Phys. Lett. A **213**, 155 (1996).
[20] Y. Liu and P. Davis, Phys. Rev. E **61**, R2176 (2000).
[21] S. Sano, A. Uchida, S. Yoshimori, and R. Roy, Phys. Rev. E **75**, 016207 (2007).
[22] K. Yoshimura, Phys. Rev. E **60**, 1648 (1999).
[23] S. Sundar and A. A. Minai, Phys. Rev. Lett. **85**, 5456 (2000).
[24] W. M. Tam, F. C. M. Lau, and C. K. Tse, IEEE Trans. Circuits Syst. **51**, 1868 (2004).
[25] L. Kocarev and U. Parlitz, Phys. Rev. Lett. **74**, 5028 (1995).
[26] W. H. Kye, M. Choi, C. M. Kim, and Y.-J. Park, Phys. Rev. E **71**, 045202(R) (2005).
[27] Y. Chembo Kouomou, P. Colet, L. Larger, and N. Gastaud, Phys. Rev. Lett. **95**, 203903 (2005).
[28] B. Dorizzi, B. Grammaticos, M. Le Berre, Y. Pomeau, E. Ressayre, and A. Tallet, Phys. Rev. A **35**, 328 (1987).
[29] J. Doyne Farmer, Physica D **4**, 366 (1982).
[30] R. Vicente, J. Daudén, P. Colet, and R. Toral, IEEE J. Quantum Electron. **41**, 541 (2005).
[31] M. W. Lee, L. Larger, V. Udaltsov, E. Genin, and J.-P. Goedgebuer, Opt. Lett. **29**, 325 (2004).
[32] R. Hegger, M. J. Bünner, H. Kantz, and A. Giaquinta, Phys. Rev. Lett. **81**, 558 (1998).
[33] V. S. Udaltsov, L. Larger, J.-P. Goedgebuer, A. Locquet, and D. S. Citrin, J. Opt. Technol. **72**, 373 (2005).
[34] C. Robilliard, E. H. Huntington, and J. G. Webb, IEEE Trans. Circuits Syst. **53**, 722 (2006).
[35] W. H. Kye, M. Choi, S. Rim, M. S. Kurdoglyan, C. M. Kim, and Y.-J. Park, Phys. Rev. E **69**, 055202(R) (2004).