Electro-optic phase chaos systems with an internal variable and a digital key

Romain Modeste Nguimdo[1,2*] **and Pere Colet**[2]

[1]*Applied Physics Research Group, Vrije Universiteit Brussel, 1050 Brussels Belgium*
[2]*Instituto de Física Interdisciplinar y Sistemas Complejos, IFISC (CSIC-UIB),Campus*
Universitat de les Illes Balears, E-07122 Palma de Mallorca, SPAIN.

** Romain.Nguimdo@vub.ac.be*

Abstract: We consider an electro-optic phase chaos system with two feedback loops organized in a parallel configuration such that the dynamics of one of the loops remains internal. We show that this configuration intrinsically conceals in the transmitted variable the internal delay times, which are critical for decoding. The scheme also allows for the inclusion, in a very efficient way, of a digital key generated as a long pseudorandom binary sequence. A single digital key can operate both in the internal and transmitted variables leading to a large sensitivity of the synchronization to a key-mismatch. The combination of intrinsic delay time concealment and digital key selectivity provides the basis for a large enhancement of the confidentiality in chaos-based communications.

OCIS codes: (250.0250,060.0060,140.0140,190.0190).

References and links

1. "Feature Section on Optical Chaos and Applications to Cryptography," edited by S. Donati and C.R. Mirasso, *IEEE J. Quantum Electron.* **38**, 1138-1184 (2002).
2. R. Lavrov, M. Peil, M. Jacquot, L. Larger, V. Udaltsov, and J. Dudley, "Electro-optic delay oscillator with nonlocal nonlinearity: Optical phase dynamics, chaos, and synchronization," *Phys. Rev. E* **80**, 026207/1-9 (2009).
3. J. P. Goedgebuer, L. Larger, and H. Porte, "Optical cryptosystem based on synchronization of hyperchaos generated by a delayed feedback tunable laser diode," *Phys. Rev. Lett.* **80**, 2249-2252 (1998).
4. L. Larger, J. P. Goedgebuer, and F. Delorme, "Optical encryption system using hyperchaos generated by an optoelectronic wavelength oscillator," *Phys. Rev. E* **57**, 6618-6624 (1998).
5. A. Argyris, D. Syvridis, L. Larger, V. Annovazzi-Lodi, P. Colet, I. Fischer, J. Garcia-Ojalvo, C.R. Mirasso, L. Pesquera, K.A. Shore, "Chaos-based communications at high bit rates using commercial fibre-optic links," *Nature* **438**, 343-346 (2005).
6. R. Lavrov, M. Jacquot, L. Larger, "Nonlocal nonlinear electro-optic Phase dynamics demonstrating $10Gbs/s$ chaos communications," *IEEE J. Quantum Electron.* **46**, 1430-1435 (2010).
7. X. Li, W. Pan, B. Luo, and D. Ma, "Mismatch robustness and security of chaotic optical communications based on injection-locking chaos synchronization," IEEE J. Quantum Electron. **42**, 953-960 (2006).
8. Y. Chembo Kouomou, P. Colet, N. Gastaud and L. Larger, "Effect of parameter mismatch on the synchronization of semiconductor lasers with electrooptical feedback," *Phys. Rev. E* **69**, 056226/1-15 (2004).
9. V.S. Udaltsov, J.-P. Goedgebuer, L. Larger, J.-B. Cuenot, Pascal Levy, W.T. Rhodes, "Cracking chaos-based encryption systems ruled by nonlinear time delay differential equations," *Phys. Lett. A* **308**, 54-60 (2003).
10. S. Ortín, J. Gutiérrez, L. Pesquera, and H. Vasquez, "Nonlinear dynamics extraction for time-delay systems using modular neural networks synchronization and prediction," *Physica A* **351**, 133-141 (2005).
11. C. R. Mirasso, P. Colet, and P. García-Fernández, "Synchronization of Chaotic Semicondcutor Lasers: Application to Encoded Communications," *Phot. Tech. Lett.* **8**, 299-301 (1996).
12. L. Larger, J. Goedgebuer, and V. Udaltsov, "Ikeda-based nonlinear delayed dynamics for application to secure optical transmission systems using chaos," *Comptes Rendus Physique* **5**, 669-681 (2004).
13. M. C. Soriano, P. Colet, and C. R. Mirasso, "Security Implications of Open- and Closed-Loop Receivers in All-Optical Chaos-Based Communications," *IEEE Photon. Technol. Lett.* **21**, 426-428 (2009).

14. R. M. Nguimdo, P. Colet, and C. R. Mirasso, ”Electro-optic delay devices with double feedback,” *IEEE J. Quantum Electron.* **46**, 1436-1443 (2010).
15. U. Leonora, M. Santagiustina, and V. Annovazzi-Lodi, ”Enhancing chaotic communication performances by Manchester coding”, IEEE Phot. Tech. Lett. **20**, 401-403 (2008).
16. V. Z. Tronciu, C. Mirasso, P. Colet, M. Hamacher, M. Benedetti, V. Vercesi, V. Annovazzi-Lodi, “Chaos Generation and Synchronization Using an Integrated Source With an Air Gap’ ’, IEEE J. Quantum Electron. **46**, 1840-1846 (2010).
17. R. Hegger, M. J. Bünner, H. Kantz and A. Giaquinta, ”Identifying and modeling delay feedback systems,” Phys. Rev. Lett. **81**, 558-561 (1998).
18. M.D. Prokhorov, V.I. Ponomarenko, A.S. Karavaev, B.P. Bezruchko, ”Reconstruction of time-delayed feedback systems from time series,” Physica D **203**, 209-223 (2005).
19. L. Zunino, M. C. Soriano, I. Fischer, O. A. Rosso, and C. R. Mirasso, ”Permutation-information-theory approach to unveil delay dynamics from time-series analysis,” Phys. Rev. E **82**, 046212/1-9 (2010).
20. D. Rontani, A. Locquet, M. Sciamanna, and D. S. Citrin, ”Loss of time-delay signature in the chaotic output of a semiconductor laser with optical feedback,” Opt. Lett. **32**, 2960 (2007).
21. D. Rontani, A. Locquet, M. Sciamanna, D. S. Citrin, and S. Ortin, ”Time-Delay Identification in a Chaotic Semiconductor Laser With Optical Feedback: A Dynamical Point of View,” IEEE J. Quantum Electron. **45**, 879-891 (2009).
22. R. M. Nguimdo, M. C. Soriano, and P. Colet, ”Role of the phase in the identification of delay time in semiconductor lasers with optical feedback,” Opt. Lett. **36**, 4332-4334 (2011).
23. R. M. Nguimdo, G. Verschaffelt, J. Danckaert, and G. Van der Sande, ”Loss of time-delay signature in chaotic semiconductor ring lasers,” Opt. Lett. **37**, 2541-2544 (2012).
24. R. Lang and K. Kobayashi, ”External Optical Feedback Effects on Semiconductor Injection Laser Properties”,IEEE J. Quantum Electron. **16**, 347 (1980)
25. J. Hizanidis, S. Deligiannidis, A. Bogris, and D. Syvridis, “Enhancement of Chaos Encryption Potential by Combining All-Optical and Electrooptical Chaos Generators”, *IEEE J. Quantum Electron.* **46**, 1642-1649 (2010).
26. H. C. Wang, K. P. Ho, H. K. Chen, and H. C. Lu, J. Lightw. Technol.” Phase and Amplitude Responses of Narrowband Optical Filter Measured by Microwave Network Analyzer”, **24**, 5075 (2006)
27. L. Zimmermann, K. Voigt, G. Winzer, K. Petermann, and C. M. Weinert, ”C-Band Optical 90^o-Hybrids Based on Silicon-on-Insulator 4×4 Waveguide Couplers”, IEEE Photon. Technol. Lett. **21** (3), 143 (2009).
28. R. M. Nguimdo, P. Colet, L. Larger and L. Pesquera, ”Digital Key for Chaos Communication Performing Time Delay Concealment,” Phys. Rev. Lett. **107**, 034103/1-4 (2011).
29. R. M. Nguimdo, R. Lavrov, P. Colet, M. Jacquot, Y. K. Chembo, and L. Larger, ”Effect of fiber dispersion on broadband chaos communications implemented by electro-optic nonlinear delay phase dynamics,” *J. Lightwave Technol.* **28**, 2688-2616 (2010).
30. A. Argyris, E. Grivas, M. Hamacher,A. Bogris, and D. Syvridis, ”Chaos-on-a-chip secures data transmission in optical fiber links,” *Optics Express*, vol. **18**, 5188-5198, 2010.
31. K. Pyragas, ”Synchronization of coupled time-delay systems: Analytical estimations,” *Phys. Rev. E* **58**, 3067-3071 (1998).

1. Introduction

The possibility of encoding and decoding multi-gigabit sensitive data using broadband chaos, has been demonstrated theoretically [1, 2], experimentally [3, 4] and in realistic installed networks [5, 6]. For this paradigm of communications, security relies mainly on the difficulty of identifying the emitter parameters necessary to build an adequate receiver which can synchronize with it [7, 8]. For this purpose, flexibility and parameter concealment are necessary to achieve a good degree of security. In particular, the systems usually considered for chaos-based communications leverage on delay to generate high dimensional chaotic carriers on which the message is encoded. The concealment of the delay time is of great interest because, in some systems, its identification is enough to reconstruct the underlying chaotic dynamics [9, 10]. In other systems, e.g. [2, 11–16], while breaking the delay time does not directly allows to hack the message, it poses a security thread since the key space dimension (a sort of equivalent to a digital key size) is reduced, exposing the systems to brute-force-attacks. Unfortunately, it has been found that the delay time can be readily identified in these systems by applying statistical techniques to the transmitted signal [10, 17–19].

There has been several proposals to overcome this drawback. For instance, in Fabry-Perot semiconductor lasers with optical feedback it has been suggested that the time-delay signatures can be eliminated if the delay is chosen close to the relaxation period of the laser operating with moderate feedback [20, 21]. In this situation statistical quantifiers computed from the intensity of the transmitted field fail to identify the delay time. However it has been recently shown that applying the same statistical techniques to the phase dynamics time-delay signatures can be successfully retrieved due to the correlation between the phase and its delayed version in the dynamics [22]. A more sophisticated technique to conceal the delay time has been introduced recently leveraging on bidirectional semiconductor ring lasers in which the cross-feedback between the counter-propagating modes allows an efficient concealment of time-delay signatures both in intensity and phase time series [23].

In optoelectronic systems [2,12,14], attempts to conceal the delay time by choosing it close to a characteristic time of the system, such as the fast time-scale of the filter, will not be successful since in this parameter region the system is not chaotic. In a first attempt to conceal the delay time in electro-optical systems, a cascaded system consisting of a combination of an all-optical system [24] and opto-electronic phase-chaos system [2] has been proposed [25]. The results for the statistical quantifiers computed from the intensity time series shows that it is possible to conceal the time delay associated to the electro-optical system. However, as more sophisticated devices such as an optical 90^o hybrid coupler [26, 27] can allow to detect the amplitude and the phase simultaneously, the approach of Ref. [22] can be used in this case to retrieve all the time delays since the overall transmitted phase is just a linear superposition of the all-optical and electro-optical system phases. Furthermore, the cascaded system becomes less chaotic than the original phase chaos system [2] for large values of the overall loop gain ($\gtrsim 3$), rendering therefore the delay identification more vulnerable.

To provide better security to chaos-based communications, we have suggested recently [28] an advanced scheme that integrates a digital key in a phase-chaos electro-optical delay system consisting of two delay chains. The digital key allows to conceal the delay time in the phase dynamics, it adds a significant degree of flexibility to the system and, moreover, it increases the key space dimensionality, avoiding another typical limitation of hardware cryptography, namely the fact that its parameter space dimension is usually relatively low compared to algorithmic cryptography. Furthermore, the non-linear mixing of chaos and the digital key allows also to conceal the key. In the scheme introduced in [28] each delay chain has two electro-optic phase modulators (PM) seeded by a continuous-wave semiconductor laser. In each chain the first PM is driven by an external signal (the digital key in one of the chains and the message to be encoded in the other) while the second PM is driven by the output of the other chain. Each chain also includes a fiber delay line, generating a delay T_i, and an imbalanced Mach-Zehnder interferometer with differential delay δT_i. The Mach-Zehnder interferometer transforms in a nonlinear way the phase variations into intensity variations, which are finally detected by a photodiode. The electrical output of the photodiode after amplification is the input for the phase modulation of the other chain. Therefore the two delay chains operate in a serial configuration, and can be viewed as part of an overall delay loop. In this configuration time-delay concealment occurs only when the digital key is present and operates at a bit rate above a threshold given by the differential delay time of the chain in which the key is introduced.

In this work we introduce, and study theoretically and numerically, a new system with two delay loops that operate in parallel so that only the output of one loop is transmitted to the receiver while the other loop remains internal. At a difference with [28] this configuration allows to conceal the internal time delays which are critical for decoding without the need for a external digital key. As we will show below, this intrinsic concealment capability comes from the fact that when loops are coupled in parallel and each loop has a different differential delay time the dynamics of the internal loop is uncorrelated to the transmitted signal. This is a

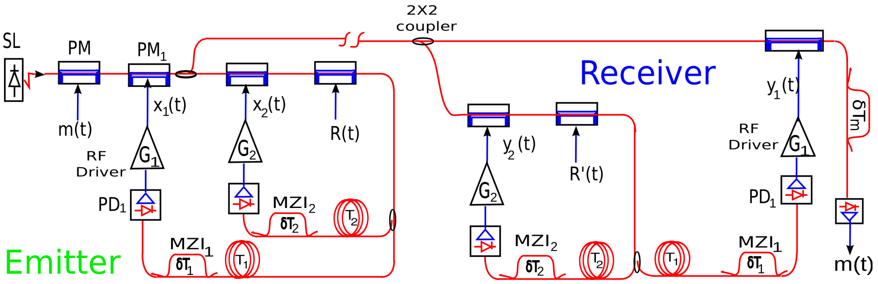

Fig. 1. Transmitter and receiver setup in the parallel configuration: SL: semiconductor laser, PM: phase modulator, MZI: imbalanced Mach-Zehnder interferometer, PD: photodiode, $x_1(t)$ and $x_2(t)$ are the dimensionless output voltages of the RF drivers for the external and the internal loops while $R(t)$ and $m(t)$ are the pseudo-random bit sequence and message, respectively. Sub-index 1 refers to the loop whose output is transmitted while 2 refers to the internal loop.

mechanism not present in the serial configuration in which the dynamical variables describing both loops are always correlated so that without digital key all the delay times can be readily identified in the transmitted signal.

On the downside, while in the serial scheme synchronization between a matched emitter and receiver pair is always achieved (unconditional synchronization) [28], in the parallel configuration considered here the fact that the internal variable is not transmitted implies that it must be regenerated at the receiver. In this situation synchronization is not always possible even in the ideal case of no mismatch between emitter and receiver. Nevertheless we show that if the gain of the internal loop is not too large an excellent degree of synchronization can be achieved.

Last but not the least, the new system also allows for the introduction of a digital key. While it is not required for time delay concealment, it is still useful to increase the parameter space. When included, the digital key plays a critical role in synchronization. In fact it turns out that the new system based on parallel loops is five times more sensitive to a key-mismatch than the serial system considered in [28] thus increasing the security.

2. System

The proposed setup is illustrated in Fig. 1. Both emitter and receiver consist of two nonlinear delayed differential processing loops, connected in parallel. The sub-indices $i = 1,2$ refer to a given loop. An electro-optic phase modulator (PM$_1$) seeded by a continuous-wave (CW) telecom semiconductor laser (SL) is phase-modulated by a voltage proportional to $x_1(t)$. The output of PM$_1$ is then split into two parts. One part is sent to the receiver while the second part is successively phase modulated by a voltage proportional to $x_2(t)$ and by the digital key $R(t)$, generated as a Pseudo-Random Bit Sequence (PRBS). After the double phase modulation the resulting optical signal is divided into two parts. Each part is fed to a fiber delay line which delays the signal by a time T_i and then fed to an Mach-Zehnder interferometer (MZI$_i$) with imbalance time δT_i, which converts phase variations into intensity variations. The intensity variations are detected by a photodiode (PD$_i$) and amplified by an RF driver with an effective gain G$_i$. The output of each amplifier, proportional to x_i, is applied to the respective RF electrode of PM$_i$ to close the loop i. The message $m(t)$ is encoded as an additional phase modulation using another PM placed in between the SL and PM$_1$ (as shown in Fig. 1) or alternatively just after PM$_1$ and prior to the split of the signal to be transmitted to the receiver. At this point we would like to note the following points: first, only the output of PM$_1$ is transmitted to the receiver, so loop 2 can be considered as internal. Second, a total of four phase modulations (two chaotic proportional to $x_1(t)$ and $x_2(t)$ + pseudorandom + message) are successively applied to the optical signal delivered at the SL output before its undergoes phase-to-intensity conversion. Third, this system requires less components than the previous one [28] since it uses a single light source for emitter-receiver system instead of three.

This set-up can be experimentally implemented using similar components as the original experimental set-up for electro-optical phase chaos [2, 6] although the implementation of the double loop requires two additional PMs and an additional MZI in both emitter and receiver. Still, as stated before, this configuration requires less components as the serial configuration [28].

The dynamical model can be described as follows. The electronic bandwidth of the loop is assumed to result from two cascaded linear first-order low-pass and high-pass filters. Considering the filter output voltages $V_i(t)$ and proceeding as in [2, 29], the emitter dynamics can be described by the dimensionless variables $x_i(t) = \pi V_i(t)/(2V_{\pi,i})$ where $V_{\pi,i}$ is the half-wave voltage of the modulator PM$_i$

$$x_i + \tau_i \frac{dx_i}{dt} + \frac{1}{\theta_i} u_i = G_i \cos^2 \left[\Delta(x_1 + x_2)_{T_i} + \Delta(R+m)_{T_i} + \phi_i\right], \tag{1}$$

where $du_i/dt = x_i$, $\Delta(F)_{t_0} = F(t-t_0) - F(t - t_0 - \delta t_0)$ and ϕ_i is the static offset phase of MZI$_i$. For numerical simulations, we consider the key physical parameters arbitrary chosen, within the range of experimentally accessible values [2, 28], as follows: $T_1 = 15$ ns and $T_2 = 17$ ns, $\tau_1 = 20$ ps, $\tau_2 = 12.2$ ps, $\theta_1 = 1.6$ μs, $\theta_2 = 1.6$ μs, $\delta T_1 = 510$ ps, $\delta T_2 = 400$ ps, $\phi_1 = \pi/4$, $\phi_2 = \pi/8$, $G_1 = 5$ and $G_2 = 3$. These parameters have been used for the original setup in [2, 6]. In practice the overall loop gain is limited, although values as large as 6 can be achieved.

3. Delay Time Concealment

The delay time can be extracted using the standard delay time identification techniques, e.g., autocorrelation function $C(s)$, delayed mutual information (DMI), extrema statistics and filling factor [17–19]. Out of those, $C(s)$ and DMI are robust to noise perturbations and therefore are suitable to crack the time delay in practical situations. For a time series $x(t)$, $C(s)$ is defined as

$$C(s) = \frac{\langle [x(t) - \langle x(t)\rangle] [x_s(t) - \langle x(t)\rangle]\rangle}{[\langle x(t) - \langle x(t)\rangle\rangle]^2}, \tag{2}$$

where $x_s(t) = x(t-s)$ and $\langle ...\rangle$ stands for the time average. The DMI measures the information on $x(t)$ that can be obtained by observing $x_s(t)$

$$DMI(s) = \sum_{x(t), x_s(t)} p(x(t), x_s(t)) \ln \frac{p(x(t), x_s(t))}{p(x(t)) p(x_s(t)))}, \tag{3}$$

where $p(x(t))$ is the probability distribution function of $x(t)$ while $p(x(t), x_s(t))$ is the joint probability distribution function.

We do not take into account the message in this section ($m = 0$). The relevant delay times for the model are T_1, $T_1 + \delta T_1$, T_2 and $T_2 + \delta T_2$. Figure 2 displays the autocorrelation (a) and the DMI (b) without (solid line) and with a PRBS of amplitude $\pi/2$ at 3 Gb/s (dashed line), computed from a long series for $x_1(t)$. Without PRBS, two relevant peaks are found both in the autocorrelation and in the DMI at delay times T_1 and $T_1 + \delta T_1$ as expected. What is more relevant is that no peak is found around the internal loop delay time positions, T_2 and $T_2 + \delta T_2$. We have also checked that using the time distribution extrema and the filling factor methods

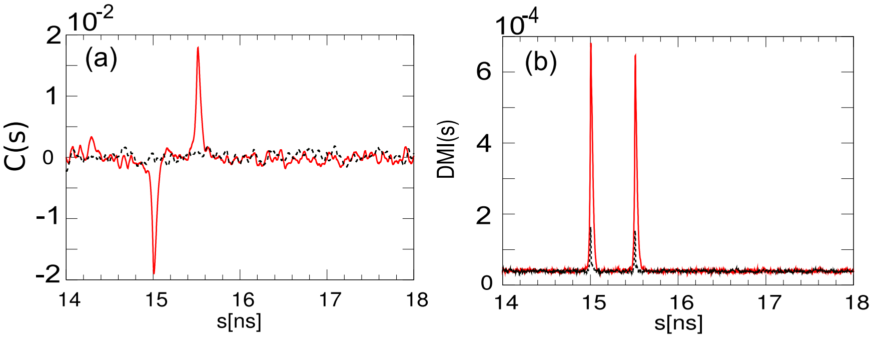

Fig. 2. Autocorrelation function $C(s)$ (a) and delayed mutual information DMI(s) (b) of $x_1(t)$ without PRBS (red line), and with a PRBS of amplitude $\pi/2$ at 3 Gb/s (black). A time series of length 10 μs with 10^7 data points was used.

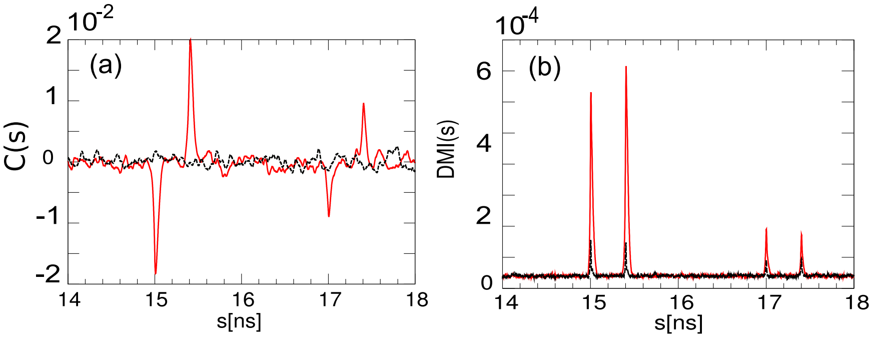

Fig. 3. Autocorrelation function $C(s)$ (a) and delayed mutual information DMI(s) (b) of $x_1(t)$ without PRBS (red line), and with a PRBS of amplitude of $\pi/2$ at 3 Gb/s (black). Parameters as in Fig. 2 but with $\delta T_1 = \delta T_2 = 400$ ps.

these delay time signatures remain concealed. Therefore the system fully conceals the internal loop delay times even without digital key.

The mechanism behind concealment of the internal loop time delays is the fact that the transmitted signal is practically uncorrelated with the internal loop dynamics. In what follows we address this issue in detail. In the serial configuration considered in [28], the dynamical variable describing one of the chains is driven only by the dynamical variable of the other chain delayed in time. The mutual driving through feedback generates a strong dynamical dependence that leads to a large correlation between the two variables. Therefore it is possible to unveil all the delay times by computing the quantifiers from only one variable. On the contrary, the parallel configuration considered here, has two particular characteristics that allow for decorrelation between the internal and the external variables. The first one is that the dynamics of each loop, besides being driven by the feedback from the other loop, includes self-feedback. This, by itself, would not be enough to preclude correlations since, as the RHS of Eq. (1) shows, both x_1 and x_2 are driven by $x_{\rm sum} = x_1 + x_2$. The second characteristic is that the loops are driven by a differential delay $\Delta(x_{\rm sum})_{T_i} = x_{\rm sum}(t - T_i) - x_{\rm sum}(t - T_i - \delta T_i)$. For loop i, the differential delay mixes $x_{\rm sum}$ at two different times separated by δT_i. If δT_1 differs from δT_2 by an amount larger than the autocorrelation time of $x_{\rm sum}$, then the result of the mixing in MZI$_1$ is practically uncorrelated from the one obtained in MZI$_2$. As a consequence in Eqs. (1), x_1 and x_2 are driven by effectively uncorrelated chaotic signals. Notice that if each loop instead of having a differential delay feedback involving two times T_i and $T_i + \delta T_i$ it had single delay time T_i, then one of the variables would be correlated with the other shifted in time by $T_1 - T_2$. Should that be the case, then the internal delays would appear in the statistical indicators of the transmitted signal. Thus differential feedback in each loop is necessary and furthermore the differential delay time of both loops must be different. Still, by itself, this is not sufficient, since in the serial configuration considered in [28] both dynamical variables are always strongly correlated despite the presence of different differential delay times. The interplay between the self-feedback and cross-feedback together with the presence of two different differential delays is what leads to decorrelation between internal and transmitted variables allowing for delay concealment.

To further discuss this issue within a mathematical framework, we consider the Fourier transform of Eqs. (1),

$$X_i(\omega)\left(1 + j\omega\tau_i + \frac{1}{j\omega\theta_i}\right) = G_i e^{-j\omega T_i}\mathbf{FT}\Big\{\cos^2\left[\bar{\Delta}(x_1 + x_2)_{\delta T_i} + \bar{\Delta}(R)_{\delta T_i} + \phi_i\right]\Big\}, \tag{4}$$

where $j^2 = -1$, $\bar{\Delta}(F)_{\delta t_0} = F(t) - F(t - \delta t_0)$ and $\mathbf{FT}\{z\}$ stands for the Fourier transform of z. For $\delta T_1 = \delta T_2$ and $\phi_1 = \phi_2$, it turns out that

$$\frac{X_1(\omega)}{X_2(\omega)} = \frac{G_1\left(1 + j\omega\tau_2 + \frac{1}{j\omega\theta_2}\right)}{G_2\left(1 + j\omega\tau_1 + \frac{1}{j\omega\theta_1}\right)}\exp\left[-j\omega(T_1 - T_2)\right]. \tag{5}$$

Equation (5) establishes a linear relationship between x_1 and x_2. Consequently information on the internal variable dynamics can be easily retrieved from the transmitted variable $x_1(t)$ and therefore for $\delta T_1 = \delta T_2$ one should expect that none of the time delays is concealed. And as shown in Eq. (5) this is certainly the case even if T_1 is different from T_2. In fact, even considering different values for the offset phases, $\phi_1 \neq \phi_2$, we have numerically found that the delay times can be identified if $\delta T_1 = \delta T_2$. The numerical results for the autocorrelation and the DMI for $\delta T_1 = \delta T_2 = 400$ ps, $\phi_1 = \pi/4$ and $\phi_2 = \pi/8$ computed from the transmitted variable x_1 are shown in Fig. 3. For this specific case, we found that the maximum of the cross-correlation between x_1 and x_2 takes place at $T_2 - T_1$ (as predicted) and is quite large, 0.7. Peaks at T_2 and $T_2 + \delta T_2$ are apparent. Clear peaks also appear at $T_2 - T_1$ (out of the figure range). In fact, while typically the delay time signature is reduced when increasing the overall loop gain (which increases the complexity of the chaos), for $\delta T_1 = \delta T_2$, the delay time can always be identified even for $G_1 = G_2 = 15$, way beyond experimental limits.

Figure 4 (a) shows the autocorrelation function for the variable $x_{\text{sum}} = x_1 + x_2$ for the parameters considered in Fig. 2. For times above 40 ps the autocorrelation is smaller than 0.1. Figure 4 (b) shows the cross-correlation between x_1 and x_2 as function of the relative mismatch in the differential delay times, $\xi = (\delta T_2 - \delta T_1)/\delta T_1$. When the feedback phases are identical the cross correlation starts at 1 for $\xi = 0$ as one can expect from the relationship given by Eq.(5). If the feedback phases are different, x_1 and x_2 are still strongly correlated at $\xi = 0$. As the difference between δT_2 and δT_1 is increased the cross correlation decreases and it finally decays to zero when this difference becomes of the order of the autocorrelation time for the variable x_{sum}. In practice, negligible values for the cross correlation are found for $|\xi|$ larger than 10%.

This result is to be compared with the one shown in Fig. 5 for the dependence of the concealment on the mismatch in the differential delay times. It turns out that as $|\xi|$ increases the peak sizes both in C(s) and DMI(s) decrease, achieving full concealment for a mismatch greater than 20%. In particular, the delay time signature is completely lost in $C(s)$ already at a 10% mismatch in correspondence with the decay time of the autocorrelation function while the DMI decays even faster to a residual value, which, although small, remains distinguishable all the way up to 20% mismatch. The reason for this larger range of detection capability is that mutual

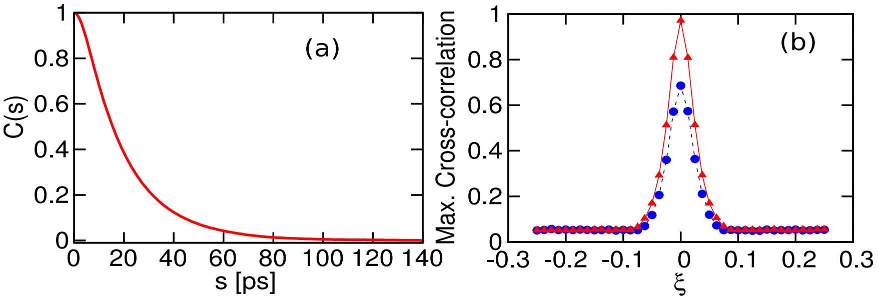

Fig. 4. a) Autocorrelation function $C(s)$ for the variable $x_{\mathrm{sum}}(t) = x_1(t) + x_2(t)$ considering the same parameters as in Fig. 2. b) Cross correlation between $x_1(t)$ and $x_2(t)$ as function of the mismatch in the differential delay time $\xi = (\delta T_2 - \delta T_1)/\delta T_1$ for (●) $\phi_1 = \pi/4$ and $\phi_2 = \pi/8$ and (△) $\phi_1 = \phi_2 = \pi/4$, considering $\delta T_1 = 400$ ps.

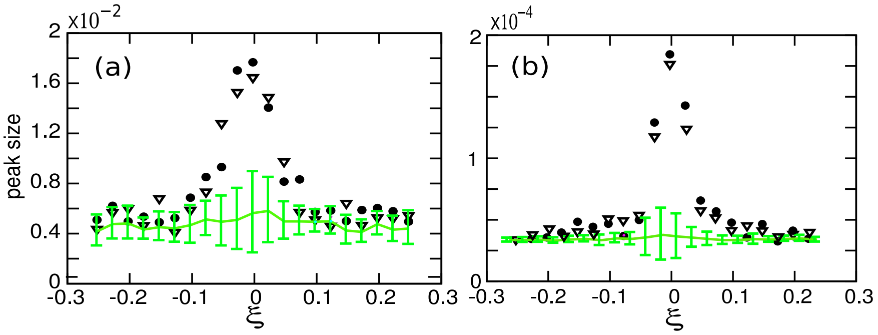

Fig. 5. Absolute value of the peaks in $C(s)$ (a), and DMI (b), at T_2 (●), $T_2 + \delta T_2$ (▽) as a function of mismatch $\xi = (\delta T_2 - \delta T_1)/\delta T_1$ considering $\delta T_1 = 400$ ps. Solid line and bars correspond to the background mean value and standard deviation. A series of length 267 times T was used.

information measures the relationship between variables beyond a linear correlation. In any case, for a differential delay mismatch above 20% not even mutual information is capable of finding traces of the internal delay times in the transmitted signal.

We finally discuss the effect of the addition of a PRBS in the concealment of the delay times of the external loop, T_1 and $T_1 + \delta T_1$. As shown in Fig. 2 the addition of PRBS successfully conceals them for the autocorrelation function [Fig. 2 (a)] but not for the DMI [Fig. 2 (b)] (although the size of the peaks is significantly reduced). The fact that the PRBS does not completely suppress these peaks can be understood as follows. Without PRBS the size of the peaks signaling T_1 and $T_1 + \delta T_1$ is stronger than in the case of the serial configuration for the same parameters [28]. This indicates that the relationship between $x_1(t)$ and its delayed version for the parallel configuration is stronger than for the serial one. The effective amplitude of the chaos driving the nonlinear term in Eqs. (1) can be twice as large as that of the serial configuration since the signal delivered by the SL is successively modulated by x_1 and x_2. Since the mixing of the PRBS and the chaos is less balanced the delay time is not concealed. Despite that, the PRBS remains efficiently masked by the chaos as the cross-correlation between $x_1(t)$ and $R(t)$ is of the order of 10^{-3}.

4. Synchronization

The signal sent to the receiver is taken at the PM$_1$ output, so $x_2(t)$ has to be generated at the receiver, through an internal closed loop. This makes the receiver to operate in semi-closed loop, which is known to be very sensitive to synchronization. The quality of the synchronization depends on several factors, including the coupling strength, parameter mismatch, noise, degradation due to fiber propagation effects. The latter has been considered in [29, 30] where it is shown that compensating the losses by in-lining erbium-doped fiber amplifiers (EDFAs) every 50 km and using dispersion management techniques, one can minimize the fiber effects to the very acceptable level. Here we neglect the effect of noise fluctuations and parameter mismatch and we focus on the conditions for synchronization depending on the internal loop gain.

Considering the setup shown in Fig. 1, and proceeding in a similar way as in Ref. [28] for the serial set up, one finds that the receiver dynamics can be described by

$$y_i + \tau_i \frac{dy_i}{dt} + \frac{1}{\theta_i} v_i = G_i \cos^2 \left[\Delta(x_1 + y_2)_{T_i} + \Delta(R' + m)_{T_i} + \phi_i \right], \tag{6}$$

where $dv_i/dt = y_i$. Since the message is encoded in the phase it has to be demodulated. This is done using a standard differential phase shift keying demodulator consisting in an MZI with an imbalance delay time δT_m and a photodetector [28]. The detected power is

$$P \propto \cos^2 [\overline{\Delta}(x_1 + m - y_1)_{\delta T_m}] \tag{7}$$

The final demodulated message m' is obtained from P. In the ideal case of perfect synchronization $y_1 = x_1$ and m' reproduces the original message m.

Considering $G_2 = 0$ in Eq. (6), $y_2(t)$ decays to zero after a characteristic time $2\tau_2/[1 - \sqrt{1 - 4\tau_2/\theta_2}] \approx \theta_2$. The receiver therefore operates in open loop and consequently the synchronization is unconditional for a matched receiver as shown in [2]. This is also the case for the serial configuration [28] since its receiver always operates in open loop. Thus starting from $G_2 = 0$, and disregarding the message $m(t) = 0$, we gradually increase G_2 in order to investigate the range of G_2 for which synchronization is possible. This can be done estimating the largest conditional Lyapunov exponent (LCLE) [31] which states that the stability of the synchronization in a delayed system can be determined by looking at the growth of state vector $\delta \in \mathbb{L}$ (where $\mathbb{L}$ is a suitable space function) constructed in the interval $\left[t - T, t\right]$. Since the system has four different delay times, T_1, $T_1 + \delta T_1$, T_2, $T_2 + \delta T_2$, we should consider the largest one $T_D = T_2 + \delta T_2$. Defining $\delta_i = y_i(t) - x_i(t)$ the LCLE defined in [31] can be modified for this system as

$$\lambda_L = \lim_{t \to \infty} \frac{1}{t} \ln \left\{ \frac{\left[\int_{-T_D}^{0} \delta_1^2 (t + t') dt' \right]^{1/2}}{\left[\int_{-T_D}^{0} \delta_1^2 (t') dt' \right]^{1/2}} \right\}. \tag{8}$$

Stable synchronization occurs for $\lambda_L < 0$. By subtracting Eqs. (1) from (6) and linearizing for δ_i, one obtains

$$\delta_i + \tau_i \frac{\delta_i}{dt} + \frac{1}{\theta_i} \varepsilon_i = -G_i \Delta(\delta_2)_{T_i} \sin [2\Delta(x_1 + x_2)_{T_i} + 2\Delta(R)_{T_i} + 2\phi_i], \tag{9}$$

where $d\varepsilon_i/dt = \delta_i$. Thus $\delta_1(t)$ to be used in Eq. (8) can be obtained by numerical integration of Eqs. (1) and (9). Note that λ_L depends implicitly on the feedback strengths G_1 and G_2. Synchronization between the external variables $x_1(t)$ and $y_1(t)$ is only possible if internal variables do synchronize first, i.e. $\delta_2(t) = 0$. Once $\delta_2 = 0$ the dynamics of δ_1 decays to zero as

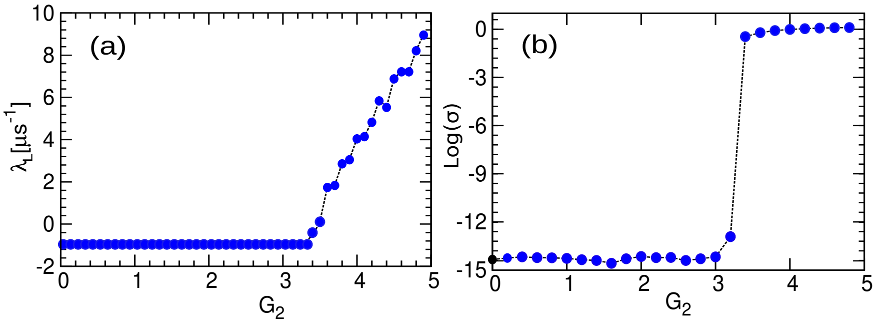

Fig. 6. (a) Largest conditional Lyapunov exponent (LCLE) versus G_2 considering $G_1 = 5$, (b) Synchronization error σ in logarithmic scale.

$\delta_1 \propto \exp[(\sqrt{1-4\tau_1/\theta_1}-1)t/2\tau_1]$. This allows to estimate the value of λ_L when synchronization takes place

$$\lambda_L = \frac{\sqrt{1-4\tau_1/\theta_1}-1}{2\tau_1} \approx -\frac{1}{\theta_1}\,. \tag{10}$$

Figure 6 (a) displays the LCLE as a function of G_2 for $G_1 = 5$ which corresponds to a relatively high gain in the external loop. Stable synchronization is found for $G_2 < G_2^{\text{th}} \approx 3.2$. Furthermore, it can be seen that for all the values of G_2 for which $x_1(t)$ and $y_1(t)$ synchronize, i.e. $G_2 < G_2^{\text{th}}$, the LCLE takes always the same value θ_1^{-1} as predicted. This also corresponds to the characteristic time that the system would take to resynchronize after an eventual desynchronization. Beyond G_2^{th}, any small perturbation $\delta_1(t)$ or $\delta_2(t)$ grows in time and therefore λ_L becomes positive indicating desynchronization between the emitter and receiver. We have found that even setting $R = 0$, the range of values for G_2 for which synchronization takes place remains the same. Similar values for the synchronization threshold G_2^{th} are obtained for other values of the external loop gain G_1 provided $G_1 > 3$. Therefore in what follows we will consider only $G_2 < G_2^{\text{th}}$.

The quality of the synchronization between $x_1(t)$ and $y_1(t)$ can also be evaluated through the root-mean square synchronization error $\sigma = \sqrt{\langle\delta_1(t)^2\rangle / \langle x_1(t)^2\rangle}$. Figure 6 (b) shows σ in logarithmic scale as function of G_2. As expected from the LCLE analysis there is perfect synchronization ($\sigma < 10^{-13}$ corresponding to the numerical accuracy) up to $G_2 = G_2^{\text{th}} \approx 3.2$. Beyond this threshold value for G_2, the synchronization rapidly degrades as indicated by an error of order 1.

5. Effect of the PRBS on Synchronization

The PRBS will play a key role in parameter space dimension if the system is sensitive to PRBS mismatch. This sensitivity can be better appreciate by considering identical parameters between the emitter and the receiver. Thus, for $R' \neq R$ the dynamics of $\delta_i(t)$ are given by

$$\begin{aligned}\delta_i + \tau_i \frac{d\delta_i}{dt} + \frac{1}{\theta_i}\varepsilon_i = -G_i \sin\left[\Delta(\delta_2)_{T_i} + \Delta(R'-R)_{T_i}\right] \\ \times \sin\left[2\Delta(x_1+y_1)_{T_i} + \Delta(\delta_2)_{T_i} + \Delta(R+R'+2m)_{T_i} + 2\phi_i\right].\end{aligned} \tag{11}$$

These equations indicate that for $R' \neq R$ synchronization is degraded both on the internal and the transmitted variables since neither δ_2 nor δ_1 decay to zero.

Figure 7 (a) shows the mean square synchronization error σ as a function of PRBS mismatch for different values of the internal loop gain G_2 while Fig. 7 (b) shows the bit error rate (BER) of

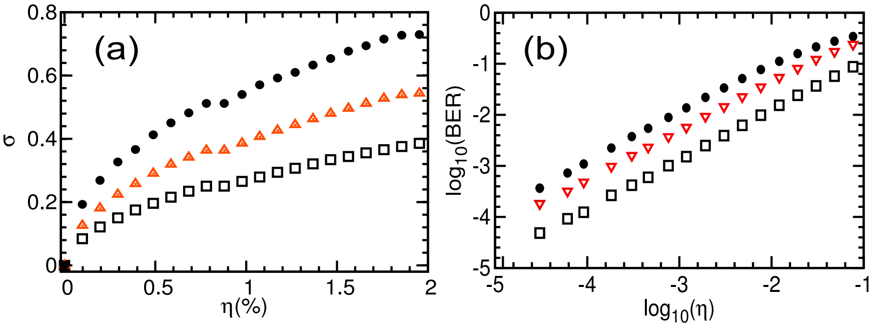

Fig. 7. Influence of the PRBS-mismatch ratio η on (a) Synchronization evaluated through the root-mean square synchronization error σ without the message, and (b) on the BER for a 10Gb/s message. We have considered a PRBS $R(t)$ of length $2^{15} = 32768$ bits generated at 3 Gb/s, $G_1 = 5$ and $G_2 = 0$ (□), $G_2 = 2$ (△), $G_2 = 3$ (●).

the recovered message. For $G_2 = 0$, there is no internal variable and therefore synchronization degradation relies on the effect of the PRBS on the transmitted variable. The synchronization error grows faster with the mismatch and just a mismatch fraction $\eta = 1\%$ in the PRBS leads to a synchronization error of 25% which corresponds to a quite poor synchronization. The BER grows linearly with the PRBS mismatch. The results obtained for $G_2 = 0$ coincide with those obtained in the serial configuration when both loops have a relatively large gain, $G_1 = G_2 = 5$ [28]. The reason for having coincident results is that in both cases the PRBS acts only on one of the variables. In fact in the serial loop configuration the PRBS acts always only on one of the variables. On the contrary, the parallel setup considered here allows for a single PRBS modulator to act simultaneously on both loops, leading to a much stronger effect as soon as the internal dynamics is switched on. As shown in Fig. 7 in the parallel configuration when increasing G_2, the degradation becomes stronger both in synchronization error and BER. As an illustration, for $G_2 = 3$ the degradation for $\eta = 0.4\%$ (i.e ≈ 131 mismatched bits in the receiver PRBS for a key $2^{15} = 32768$ bit long) is equivalent to that obtained for $\eta = 2\%$ (i.e ≈ 655 mismatched PRBS bits) when $G_2 = 0$. In other words, the PRBS mismatch sensitivity for $G_2 = 3$ is 5 times larger than that obtained in the serial configuration with $G_2 = 5$ [28]. Using PRBS of different lengths leads to similar results, namely, the relevant parameter is the fraction of mismatched bits between emitter and receiver PRBS. Note that for bit rates lower than $1/\delta T_i$, the effect of the PRBS is largely reduced. This is because at those low bit rates $R(t)$ and $R(t-\delta T_i)$ have the same value most of the time. The same happens for $R'(t)$ and $R'(t-\delta T_i)$. Therefore $\Delta(R'-R)_{T_i} = R'(t-T_i) - R'(t-T_i-\delta T_i) - R(t-T_i) + R(t-T_i-\delta T_i)$ vanishes even if R and R' are different.

6. Conclusions

We have studied an electro-optic phase chaos system with digital key based on two parallel electro-optic phase-chaos loops. This allows for the generation of two phase-chaos variables, one of which is transmitted to the receiver while the other remains internal. A suitable receiver is organized in a semi-closed loop configuration since it contains both an open loop for the transmitted variable and a closed one to regenerate the internal variable. Synchronization takes place even for moderate values of the internal loop gain up to $G_2 \approx 3.2$. We have shown that the nonlinear dynamics of the system allows for a decorrelation between the internal variables and the transmitted signal so that the system intrinsically conceals the internal delay times. This was not possible in the serial configuration introduced before [28] which had to rely on an external digital key to conceal the delay times. The key ingredients for the intrinsic concealment are the parallel coupling of the loops and the operation using different differential delay feedback times for each loop.

Besides, the introduction of a digital key decreases the signature corresponding to the two delay times of the external loop although it does not completely suppress them. Interestingly, the parallel configuration allow for a single digital key to act on both dynamical variables leading to a much stronger effect on the synchronization degradation when the key is not matched as compared with the serial configuration [28]. Therefore the parallel configuration besides providing intrinsic time delay concealment also allows for the introduction of a digital key in a very effective way to increase the parameter space dimension. Both aspects contribute in a very significant way to enhance the confidentiality in chaos-based communications.

7. Acknowledgements

The authors thank L. Larger for valuable discussions. Financial support from MINECO, Spain, and Feder under Projects FIS2007-60327 (FISICOS) and TEC2009-14101 (DeCoDicA) and by the EC Project PHOCUS (FP7-ICT-2009-C-240763) is acknowledged. R.M.N. acknowledges fellowship BES-2007-14627 under the FPI program of MINECO. Also, he acknowledges the Research Foundation Flanders (FWO) for project support and fellowships, and the Belgian Interuniversity Attraction Pole Network photonics@be.