Digital key for chaos communication performing time delay concealment

Romain Modeste Nguimdo[1], Pere Colet[1], Laurent Larger[2], Luís Pesquera[3]
[1]*Instituto de Física Interdisciplinar y Sistemas Complejos, IFISC (CSIC-UIB), Campus Universitat de les Illes Balears, E-07122 Palma de Mallorca, SPAIN.*
[2]*UMR CNRS FEMTO-ST 6174/Optics Department, University of Franche-Comté, 16 Route de Gray, 25030 Besançon cedex, France*
[3]*Instituto de Física de Cantabria, (CSIC-Universidad de Cantabria), Santander E-39005,Spain*
(Dated: June 1, 2011)

We introduce a scheme that integrates a digital key in a phase-chaos electro-optical delay system for optical chaos communications. A pseudo-random binary sequence (PRBS) is mixed within the chaotic dynamics in a way that a mutual concealment is performed, e.g. the time delay is hidden by the binary sequence, and the PRBS is also masked by the chaos. Besides bridging the gap between algorithmic symmetric key cryptography and chaos-based analog encoding, the proposed approach is intended to benefit from the complex algebra mixing between a (pseudo-random) boolean variable, and another continuous time (chaotic) variable. The scheme also provides a large flexibility allowing for easy reconfigurations to communicate securely at high bit rate between different systems.

PACS numbers:

Since the emergence of experimental chaos encryption dating back to the seminal work of Cuomo *et al.* in the earlier 90's [1], proofs of principles have been extensively reported ranging from electronic, optical [2] to opto-electronic [3] systems. These last years, field demonstrations have been conducted over installed optical fiber network, involving high bit rate message, and using standard telecommunications components [4, 5]. Typically, the chaos is generated using analog systems subject to either optical or electro-optical delayed feedback. In chaos encryption there is no rigorous counterpart to the digital key of algorithmic cryptography. Confidentiality relies essentially on the hardware parameters that should be kept secret. Unfortunately, the time delay in itself, though being a very sensitive key parameter for a proper decoding, has been found to be vulnerable since it can be identified from the chaotic time series using methods such as autocorrelation function, delayed mutual information (DMI), extrema statistics and filling factor [6] even in systems with multiple delays [7]. Out of those, autocorrelation and DMI are robust to noise perturbations and therefore are suitable to crack the time delay. Still worse, under the assumption of noise-free or even of small noise, it has been shown that the underlying chaotic dynamics of some systems can be reconstructed, once the time delay is identified, using appropriate techniques such as artificial neural networks [8]. Another limit of hardware cryptography relies on the fact that its parameter space dimension (a sort of equivalent to the digital key size) is relatively low compared to algorithmic cryptography.

To circumvent these drawbacks, we propose in this Letter to implement a currently suggested principle in algorithmic cryptography, which consists in mixing different algebra when constructing the encryption algorithm [9]. The idea is to combine a pseudo-random binary sequence (PRBS) typically used in symmetric key encryption, together with an analog physical chaos, in order to provide an enhanced cryptographic security through the reciprocal concealment between the boolean pseudo-random sequence and the high dimensional continuous time chaotic motion. At this point we notice that while public-key encryption schemes have won popularity, they have drawbacks such as limited speed and non-absolute security. Thus symmetric-key algorithms are still actively pursued, including new stream cyphers [10] and cryptographic hash functions [11]. Besides, hybrid algorithms such as the PGP combine public key encryption to define a private key used for fast symmetric encryption [12].

In general chaotic communications mix the digital message and the chaotic carrier, however this mixing is quite weak and the statistical properties of the message cannot be controlled beforehand, thus the masking of the chaotic carrier statistical properties is quite limited. Through the introduction of an amplitude-balanced entropy mixing between a PRBS and a chaotic generation process, we perform an efficient entropy amplification for the resulting carrier even in absence of any message. As a consequence, this approach proposes a solution both for the problem of the introduction of an efficient digital key in chaos communications, as well as for the problem of time delay concealment. There have been indeed recently a few attempts to address separately these issues. In semiconductor lasers with optical feedback, the optical feedback phase plays an important role in the synchronization [13] thus a digital key implemented by modulating that phase was suggested [14]. In the same context, it has been also suggested [15] that time delay can be masked if chosen to be close to the laser relaxation time, however chaos complexity is weak in that regime. Systems with time delay modulation [16] proposed as alternatives to get around the time-delay extraction, are however very difficult to implement practically.

Here we propose a configuration based on a double electro-optic delayed feedback dynamics. The scheme al-

lows on one hand to integrate a digital key required for successful decryption which can be implemented as a long PRBS generated by an appropriate algorithm or as a relatively short sequence generated from a natural random process used repetitively. On the other hand, under conditions described later, the digital key conceals the delay time so that it cannot be identified using known methods. Besides the scheme, our proposal is based physically on high speed phase chaos [17] which has been recently successfully tested in a chaos communication field experiment up to 10 Gb/s [5]. Though the proposed system is inspired by the principles reported in [5], structural architecture modifications have been necessary in order to ensure the efficient achievement of our initial goal: security enhancement of chaos communication through the use of a digital key. The proposed setup is illustrated in Fig. 1. Both emitter and receiver are consisting of two similar nonlinear delayed differential processing chains, serially connected. The sub-indices $i = 1, 2$ refer a given chain. Each chain has an electro-optic phase modulator (PM) with a half-wave voltage V_π seeded by a continuous-wave (CW) telecom semiconductor laser (SL), which is phase modulated by an external signal (whether the PRBS, R, or the message m). The electrical input of the PM of a chain, is driven by the electrical output of the other chain. The PM optical output of one chain thus consists of two superimposed phase modulations, the PRBS or the message, and the nonlinear delayed differential processing performed by the other chain. The phase modulated light beam is then processed according to the delayed nonlinear dynamics of its chain. The time delay T_i is performed by a length of fiber. The nonlinear transformation is performed non locally in time [17], between the input phase and the output intensity of an Mach-Zehnder interferometer (MZI) with imbalancing δT_i which is longer than the typical time scale of the phase modulation. The intensity fluctuations are detected by an amplified broadband telecom photodiode (PD). The output electrical signal is further amplified by an RF driver, which gives the output of the processing chain serving as the electrical input for the other chain. The transmitted light beam is the output of PM_2, which contains the linearly superimposed

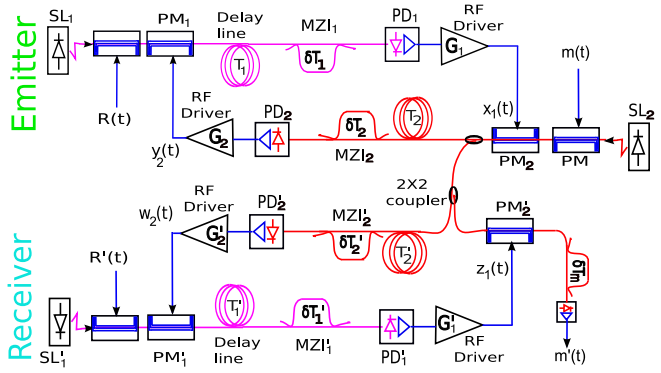

FIG. 1. (Color on line) Setup (see text).

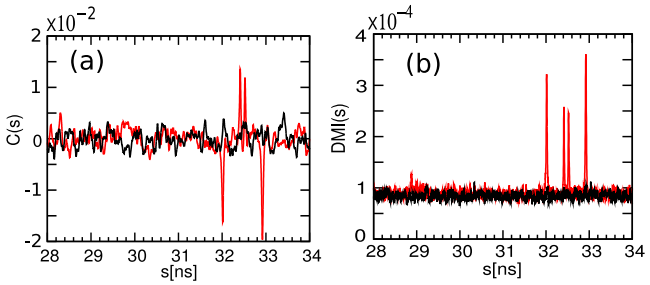

FIG. 2. (Color on line) $C(s)$ (a) and DMI (b) without PRBS (grey, red on line), and with a 3 Gb/s PRBS of amplitude $\pi/2$ (black). A 10 μs time series with 10^7 data points was used.

message in DPSK (differential phase shift keying) format.

The dynamical modeling 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 $V_1(t)$ and $V_2(t)$ and proceeding as in [17, 18], the emitter dynamics can be described by the dimensionless variables $x_1(t) = \pi V_1(t)/(2V_{\pi,1})$ and $y_2(t) = \pi V_2(t)/(2V_{\pi,2})$:

$$x_1 + \tau_1 \frac{dx_1}{dt} + \frac{1}{\theta_1} u_1 = \beta_1 \cos^2 \left[\Delta(y_2 + R)_{T_1} + \phi_1\right], \quad (1)$$

$$y_2 + \tau_2 \frac{dy_2}{dt} + \frac{1}{\theta_2} u_2 = \beta_2 \cos^2 \left[\Delta(x_1 + m)_{T_2} + \phi_2\right], \quad (2)$$

where $du_1/dt = x_1$, $du_2/dt = y_2$ and $\Delta(F)_{t_0} = F(t-t_0) - F(t-t_0-\delta t_0)$. The key physical parameters are arbitrary chosen, within the range of experimentally accessible values [17], as follows: the feedback strengths $\beta_1 = \beta_2 = 5$, the delay times $T_1 = 15$ ns and $T_2 = 17$ ns, the fast (slow) filter characteristic response times $\tau_1 = 20$ ps ($\theta_1 = 1.6$ μs) and $\tau_2 = 12.2$ ps ($\theta_2 = 1.6$ μs), the MZI imbalanced delays $\delta T_1 = 510$ ps and $\delta T_2 = 400$ ps, and the MZI static phases $\phi_1 = \pi/4$ and $\phi_2 = \pi/8$.

We first consider that no message is transmitted ($m(t) = 0$) to show the role of the PRBS in the statistical properties of the carrier $x_1(t)$. As stated before, the most robust methods to extract the time delay are the autocorrelation $C(s)$ and the DMI between the value of the variable and its time-lagged version [6]. We focus on these two methods since extrema statistics and filling factor methods are so sensitive to noise that even just a 1% noise added to the carrier prevent them to work properly. Fig. 2 displays $C(s)$ and the DMI computed from the transmitted phase proportional to $x_1(t)$, without PRBS (grey line, red on line) and with a PRBS of amplitude $\pi/2$ at 3 Gb/s (black line). In the first case both functions show peaks at $T = T_1 + T_2$, $T + \delta T_1$, $T + \delta T_2$ and $T + \delta T_1 + \delta T_2$, so that all relevant time delays can be readily identified. The delay time signature vanishes completely when the PRBS is included.

Figs. 3 a) and b) show the size of peaks found in $C(s)$ and DMI at the relevant delay times as a function of the PRBS bit rate considering an amplitude of $\pi/2$. The peaks are clearly distinguishable for zero bit rate (no

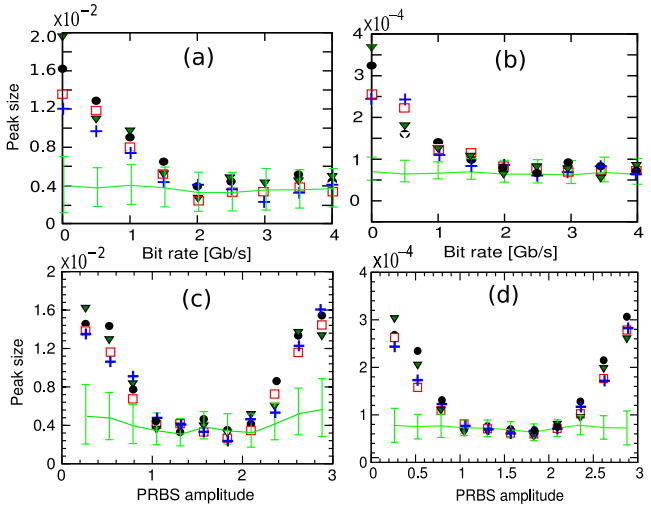

FIG. 3. (Color on line) Absolute value of the peaks in $C(s)$ (a,c), and DMI (b,d), at T (•), $T+\delta T_2$ (□), $T+\delta T_1$ (+) and $T+\delta T_1+\delta T_2$ (▼). In a) and b) the PRBS amplitude is $\pi/2$ while in c) and d) the PRBS bit rate is 3Gb/s. Solid line and bars correspond to the background mean value and standard deviation [19]. A series of length 267 times T was used.

PRBS). Increasing the bit rate, the peak size decreases. For low bit rates $R(t)$ and $R(t-\delta T_1)$ take the same value most of the time, so $\Delta(R)_{T_1}$ usually vanishes and the effect is small (see the concept of temporal non locality as introduced in [17]). Therefore the peaks both in the DMI and in $C(s)$ can still be distinguished from the background standard deviation, shown with bars in the figure [19]. When the bit rate reaches a value corresponding to the inverse of δT_1 (~ 1.97 Gb/s), $\Delta(R)_{T_1}$ is typically non zero, and the PRBS plays a key role in the dynamics, concealing the time delay peaks. The size of the peaks as function of the PRBS modulation amplitude [Figs. 3 c) and d)] is a π-periodic function associated to the periodicity of $\cos^2$ in Eq. (1). A PRBS of amplitude π has no effect since $\Delta(R)_{T_1}$ only takes values 0 or π and both are equivalent in the $\cos^2$ term. Efficient concealment occurs for amplitudes between $\pi/3$ and $2\pi/3$ approximately. This range increases increasing β.

Remarkably enough, while the PRBS conceals the delay time in the chaotic carrier $x_1(t)$, the cross-correlation between $x_1(t)$ and $R(t)$ is of the order of 10^{-3}, meaning that the digital key itself is also concealed in the chaotic carrier. This is explained by the fact that the interplay between balanced amplitudes of the chaos and a PRBS is optimizing the mutual nonlinear mixing, resulting in an efficient mutual masking of each signal by the other.

At the receiver side, decoding is performed as follows. The input phase-modulated beam is split into two paths. The long path replicates the two serial processing chains used for the encoding at the emitter, in which a synchronized PRBS is involved, thanks to the knowledge of the digital secret key. The analog secret key consists in the hardware parameters determining the devices and their exact operating conditions. The output of the two processing chains, after being inverted, serves as the electrical input of PM'_2, which is intended to cancel the carrier. The dynamics at the receiver is given by:

$$z_1+\tau_1'\frac{dz_1}{dt}+\frac{1}{\theta_1'}v_1=\beta_1'\cos^2\left[\Delta(w_2+R')_{T_1'}+\phi_1'\right], \quad (3)$$

$$w_2+\tau_2'\frac{dw_2}{dt}+\frac{1}{\theta_2'}v_2=\beta_2'\cos^2\left[\Delta(x_1+m)_{T_2'}+\phi_2'\right], \quad (4)$$

where $dv_1/dt=z_1$, $dv_2/dt=w_2$, and primes refer to the receiver parameters. The output of PM'_2 is then expected to be the phase modulation issued by the message only. It can be demodulated using a standard DPSK demodulator, consisting in an MZI with an imbalance delay time δT_m and a photodetector. The detected power is

$$P(t)\propto\cos^2\left[\Delta(x_1+m)_{\delta T_m}-\Delta(z_1)_{\delta T_m}\right]. \quad (5)$$

where in this specific case $\Delta(F)_{\delta T_m}=F(t)-F(t-\delta T_m)$. The decoded message $m'(t)$ is obtained from $P(t)$. For perfect synchronization, $z_1(t)$ is equal to $x_1(t)$, and $m'(t)$ reproduces $m(t)$. While hardware mismatch is unavoidable in practice, several field experiments [4, 5] have demonstrated that the resulting synchronization error is still acceptable. Moreover, the electro-optic phase dynamics we consider as our basis has led to the best experimental chaos synchronization quality reported so far over more than 10GHz bandwidth. The correct decoding, however, depends strongly on the matching of all the parameters, in the same way as it was already investigated in the literature [20]. The sensitivity of the decoding with respect to physical parameter mismatch is thus not revisited here. To check that the precise knowledge of the PRBS indeed brings significant additional security we consider in the following that the receiver parameters are identical to the transmitter. The differences $\delta_1(t)=z_1(t)-x_1(t)$ and $\delta_2(t)=w_2(t)-y_2(t)$ follow:

$$\delta_1+\tau_1\frac{d\delta_1}{dt}+\frac{1}{\theta_1}\varepsilon_1=-\beta_1\sin\left[\Delta(\delta_2)_{T_1}+\Delta(R'-R)_{T_1}\right]$$
$$\times\sin\left[2\Delta(y_2)_{T_1}+\Delta(\delta_2)_{T_1}+\Delta(R'+R)_{T_1}+2\phi_1\right] \quad (6)$$

$$\delta_2+\tau_2\frac{d\delta_2}{dt}+\frac{1}{\theta_2}\varepsilon_2=0 \quad (7)$$

where $d\varepsilon_1/dt=\delta_1$ and $d\varepsilon_2/dt=\delta_2$. From Eq. (7) it turns out that δ_2 decays to zero after a time of order θ_2. For $R'_{T_1}=R_{T_1}$, once δ_2 decayed to zero, the RHS of Eq. (6) vanishes so that δ_1 also decays to zero after a time of order θ_1. Therefore the receiver synchronizes perfectly to the emitter after a transient of order $\theta_1+\theta_2$. However, for a mismatched PRBS the RHS of Eq. (6) does not vanish and therefore δ_1 is finite, resulting in a degraded synchronization. Actually, for identical parameters, δ_2 decays to zero despite any eventual PRBS mismatch, thus the internal variable does synchronize. Synchronization degradation takes place on the transmitted variable.

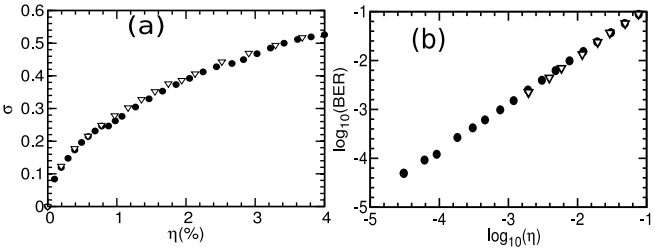

FIG. 4. Influence of PRBS-mismatch on σ (a) and on BER for a 10 Gb/s message (b). We use PRBSs of amplitude $\pi/2$ and length 2^{15} ($\bullet$) and 2^9 (∇) bits generated at 3 Gb/s.

Fig. 4(a) displays the root-mean square synchronization error $\sigma = \sqrt{\langle \delta_1(t)^2 \rangle / \langle x_1(t)^2 \rangle}$ as a function of the percentage of wrong bits η in the receiver PRBS, where $\langle\rangle$ stands for time average. σ grows fast from zero when the PRBSs differ. Even for a 1% difference in the PRBS key σ is close to 25% indicating a very poor synchronization. When synchronization is degraded, $z_1(t)$ does not replicate $x_1(t)$, and the quality of the recovered message decreases. The most relevant way to characterize this is by measuring the Bit Error Rate (BER) of the recovered message (Fig. 4(b)). The BER increases linearly with η. For a pseudorandom message of amplitude $\pi/2$ ($\approx 30\%$ of the carrier amplitude) transmitted at 10Gb/s a 1% mismatch in the PRBS leads to a BER of 0.01. Results are similar for keys of different length as shown in Fig. 4(b).

In conclusion we have shown that a digital key can be integrated with a chaos-based communication system in a way that it conceals the delay time and it is necessary for decoding. Besides bridging the gap between symmetric-key algorithmic cryptography and chaos-based encoding, the concealment of the time delay is particularly relevant to prevent from eventual eavesdropper attacks. In our phase-chaos electro-optical delay system the chaotic dynamics does not reveal the digital key so it is possible to use it in a repetitive way while concealing it. The interference generated by the two similar time delays present in our system plays a critical role in the mutual concealment. We have found that in a similar electro-optical setup for intensity chaos generation with a single delay time no concealment takes place. In our system, the effective key-space of the encryption can be defined as the product of the analog key size and the digital one. From another viewpoint, the mixing of a digital source of entropy, and an analogue one, can be viewed as an entropy amplification procedure, which is strongly relevant in terms of cryptographic security. Furthermore, the setup can be easily modified or reconfigured, both from the digital or analogue source of entropy.

On a broad perspective, as for PGP, chaotic symmetric encryption schemes as proposed here may be typically dedicated to high speed secure data transmission. Asymmetric encryption (based on algorithmic cryptography, mutually coupled optical chaos [21] or quantum key distribution [22]) could bring the complementary solution for efficient and secure (perhaps slower) secret key exchange.

Financial support from MICINN, Spain, and Feder under Projects TEC2006-10009 (PhoDeCC), FIS2007-60327 (FISICOS) and TEC2009-14101 (DeCoDicA) and by EC Project PHOCUS (FP7-ICT-2009-C-240763) is acknowledged. R.M.N. also acknowledges the fellowship BES-2007-14627 under the FPI program of MICINN.

[1] K. M. Cuomo and A. V. Oppenheim, Phys. Rev. Lett. **71**, 65 (1993).
[2] P. Colet and R. Roy, Opt. Lett. **19**, 2056, (1994); C.R. Mirasso, P. Colet, P. García-Fernández, IEEE Photon Technol. Lett.**8**, 299 (1996); V. Annovazzi-Lodi, S. Donati and A. Sciré IEEE J. Quantum Electron. **32**, 953 (1996); G. D. Van Wiggeren and R. Roy, Science, **279**, 1198 (1998).
[3] H. D. I. Abarbanel *et. al.*, IEEE J. Quantum Electron. **37**, 1301 (2001); L. Larger, J.-P. Goedegbuer, and V. S. Udalsov, C.R. de Physique 4, **5**, 681 (2004).
[4] A. Argyris *et. al.*, Nature (London) **438**, 343 (2005).
[5] R. Lavrov, M. Jacquot, L. Larger, IEEE J. Quantum Electron. **46**, 1430 (2010).
[6] M.J. Bünner *et. al.*, Phys. Lett. A **211**, 345 (1996); B. P. Bezruchko *et. al.*, Phys. Rev. E **64**, 056216 (2001); V.S. Udaltsov *et. al.*, Phys. Lett. A **308**, 54 (2003); L. Zunino *et. al.*, Phys. Rev. E **82**, 046212 (2010).
[7] M.D. Prokhorov *et al.*, Physica D **203**, 209 (2005).
[8] S. Ortín *et. al.*, Physica A **351**, 133 (2005).
[9] A. Klimov and A. Shamir in *Fast Software Encryption* chapter 1, ed. by B. Roy and W. Meier, Lect. Notes in Computer Sciences **3017**, Springer, Berlin (2004).
[10] See for example the European project eSTREAM (http://www.ecrypt.eu.org/stream).
[11] See for example the NIST call for the future SHA-3 (http://csrc.nist.gov/groups/ST/hash/sha-3/).
[12] P.R. Zimmermann, *PGP: Source code and internals*, MIT Press (1995).
[13] M. Peil *et. al.*, Phys. Rev. Lett., **88**, 174101 (2002); T. Heil *et. al.*, IEEE J. Quantum Electron. **38**, 1162 (2002).
[14] A. Bogris *et. al.*, IEEE J. Quantum Electron.**44**, 119 (2008).
[15] D. Rontani *et. al.*, IEEE J. Quantum Electron. **45**, 879 (2009).
[16] W. H. Kye, M. Choi, and C.-M. Kim, Phys. Rev. E **71**, 045202(R) (2006); C. Robilliard, E. H. Huntington, and J. G. Webb, IEEE Trans. Circuits Syst. **53**, 722 (2006); D. Rontani *et. al.*, Phys. Rev. E **80**, 066209 (2009).
[17] R. Lavrov *et. al.*, Phys. Rev. E **80**, 026207 (2009).
[18] R. M. Nguimdo *et. al.*, IEEE J. Lightwave Tech. **28**, 2688 (2010).
[19] The background mean and standard deviation are calculated using the highest 2000 spurious local maxima (i.e. excluding the peaks corresponding to real delay times).
[20] Y. K. Chembo *et. al.* Phys. Rev. E **69**, 056226 (2004).
[21] J. Scheuer and A. Yariv, Phys. Rev. Lett. **97**, 140502 (2006); M. Peil, L. Larger and I. Fischer, Phys. Rev. E **76**, 045201 (2007).
[22] N. Gisin *et. al.* Rev. Mod. Phys. **74**, 145 (2002).