IEICE Proceeding Series

Mixing of analogue and digital entropies for optical chaos communications

Laurent Larger, Romain Modeste Nguimdo, Luis Pesquera, Pere Colet

Vol. 1 pp. 332-335
Publication Date: 2014/03/17
Online ISSN: 2188-5079

2012 International Symposium on Nonlinear Theory and its Applications
NOLTA2012, Palma, Majorca, Spain, October 22-26, 2012

Mixing of analogue and digital entropies for optical chaos communications

Laurent Larger†, Romain Modeste Nguimdo‡, Luis Pesquera⋆, and Pere Colet‡

† FEMTO-ST / Optics Dept., UMR CNRS 6174, University of Franche-Comté
16 route de Gray, F-25030 Besançon cedex, France
‡ IFISC, CSIC, Universitat de les Illes Baleares, Palma de Mallorca, Spain
⋆ IFCAS, Universidad de Cantabria, Santander, Spain
Email: llarger@univ-fcomte.fr

Abstract—Security issues in optical chaos communications is still an open problem, mainly because of known time series analysis techniques that enable to recover, at least in principle, the physical parameters ruling the chaotic motion. On the basis of a recently proposed electro-optic phase chaos architecture, we propose a novel physical encryption scheme which is mixing the broadband analogue encryption of chaos communication, together with the flexibility of a numerically generated pseudo-random binary sequence. The approach is shown to provide efficient time delay concealment in the transmitted signal, which is one of the most critical physical parameter in delay-based chaos communication systems.

1. Introduction

Chaos communications appeared as a direct consequence of the possibility for synchronized chaotic motion, allowed by a suitable coupling in a Master-Slave configuration between distant emitter and receiver. Beyond the theoretical description of suitable coupling, experimental demonstrations were rapidly achieved via electronic circuits performing chaotic dynamics in 3D or 4D phase space dynamics. However, powerful parametric identification tools prevented these preliminry demonstrators for being satisfactory answers for providing a sufficient security level to this new kind of analogue encryption approach. The approach moved then to more complex dynamical motions, expecting more difficulties for eavesdroppers. Delay dynamics have been proposed with significant improvments and great expectations in terms of security and performances of chaos communications. On the one hand it provided infinite dimensional phase space together with very moderate setup complexity, and on the other hand through the physical implentation in Optics, it opened to chaos communications the very attractive transmission speed capability of modern optical telecommunications [1]. However, once again, powerfull methods for time series analysis dedicated to delay dynamics, showed that the actual high complexity of the chaotic motion could be overcome simply by using intrinsic structural simplicity of the differential equations ruling the chaotic motion. An important observation was the following: these identification methods were developed for delay dynamics parameters recovery, but their efficiency (accuracy for the identification) was strongly decreased when applied to a real chaos communication signal, i.e. a signal composed by two compounds that are nonlinear mixed through the delayed feedback loop of the oscillator. These compounds were the delay feedback (chaotic) signal, and the binary data stream injected inside the oscillation loop. Following this observation, we proposed to investigate an improved version of the standard chaos communication schemes, in which the masking signal is generated from two entropy sources: a fast one following the same optoelectronic nonlinear delayed feedback loop generating chaos, and a slightly slower one provided by simple a standard pseudo random number generators (PRBS, such as the deterministic, but broadband bit stream used in bit error testers, and obtained from feedback shift registers). The signal then is still introduced in this in the hybrid analogue and digital masking carrier, thus still a priori allowing for a standard self synchronization open loop receiver.
We will first present the physical details of the experimental setup. In a second section, we will evaluated the robustness of the generated masking carrier against the most critical time series identification step consisting in the time delay identification through autocorrelation function and averadge mutal information. In the last section we propose to conclude on impact of our methods on the next generation of chaos-based communication systems.

2. Hybrid analogue and digital encoding

We propose an experimental configuration based on a double electro-optic delayed feedback dynamics. The scheme allows on one hand to integrate a digital key used to generate a long PRBS, which would also be required by the authorized receiver for successfull decryption. On the other hand, the involved digital random sequence performs a concealment of the delay time, under conditions decribed later, so that the time delay cannot be anymore identified from the time series using known methods. Besides the scheme, our proposal is based physically on high speed phase chaos [2] which has been recently successfully tested in a chaos communication field experiment up to 10Gb/s [3]. Though the proposed system is inspired by the principles reported in [3], significant architecture mod-

ifications 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, for the emitter part (receiver can be constructed similarly to already known open loop self synchronization principle). This emitter is consisting of two similar nonlinear delayed differential processing chains, serially connected. The subindices "a" or "b" refer to elements of the same chain. In each chain, one has an electro-optic phase modulator (PM) seeded by a continuous-wave (CW) telecom semiconductor laser (SL), which is phase modulated by an external signal (whether the PRBS with a "p" subscript for the chain "a", or the data to be securely transmitted with a "d" subscript for the chain "b"). 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 lightbeam is then processed according to the delayed nonlinear dynamics of its chain. The time delay $T_{a,b}$ is performed by a cumulated length of fiber and RF cables. The nonlinear transformation is performed non locally in time [2], between the input phase and the output intensity of an imbalanced interferometer (e.g. a passive Mach-Zehnder interferometer MZI), which imbalancing $\delta T_{a,b}$ is required to be longer than the typical time scale of the phase modulation. The intensity fluctuations resulting from this nonlinear conversion of the phase modulation, are then detected by an amplified broadband telecom photodiode. 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 phase modulated lightbeam is the output of PM_b, which contains the linearly superimposed phase modulation of the message in standard DPSK (differential phase shift keying) format.

The dynamical modeling of the encoding can be described

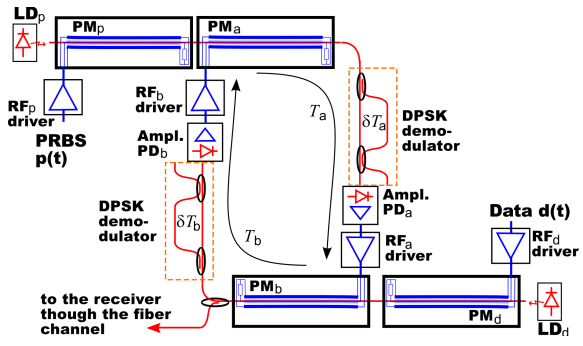

Figure 1: Electro-optic Phase delay dynamics mixed with a pseudo random bit sequence, and the data to be hidden in the mixed analogue digital entropy signal.

as follows. The electronic bandwidth of the feedback loop is assumed to result from two cascaded linear first-order

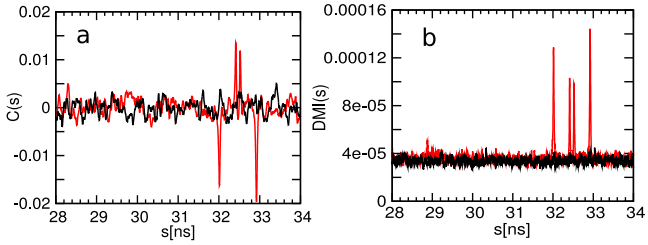

Figure 2: (Color on line) Autocorrelation function $C(s)$ (a) and delayed mutual information DMI(s) (b) of $x_{rma}(t)$ without PRBS (Grey, red on line), and with a PRBS at 3 Gbit/s (black) and with an amplitude of $\pi/2$. A time series of length 10 μs with 10^7 data points was used.

low-pass and high-pass filters. Performing a derivation similar to the one given in [2, 4], it turns out that the emitter dynamics can be described by the dimensionless output filter variables $x_{rma}(t)$ and $y_b(t)$:

$$x_{rma} + \tau_{rma}\frac{dx_{rma}}{dt} + \frac{1}{\theta_{rma}}u_{rma} = \beta_{rma}\cos^2\left[\Delta(y_{rmb})_{T_{rma}} + \Delta p_{T_{rma}} + \phi_{rma}\right],$$

$$y_{rmb} + \tau_{rmb}\frac{dy_{rmb}}{dt} + \frac{1}{\theta_{rmb}}u_{rmb} = \beta_{rmb}\cos^2\left[\Delta(x_{rma})_{T_{rmb}} + \Delta d_{T_{rmb}} + \phi_{rmb}\right],$$

where $du_{rma}/dt = x_{rma}$, $du_{rmb}/dt = y_{rmb}$ and $\Delta F_{t_0} = F(t-t_0) - F(t-t_0-\delta t_0)$. The parameters are the feedback strengths $\beta_{rma} = \beta_{rmb} = 5$, the delay times $T_{rma} = 17$ ns and $T_{rmb} = 15$ ns, the fast (slow) filter characteristic response times $\tau_{rma} = 20$ ps ($\theta_{rma} = 1.6$ μs) and $\tau_{rmb} = 12.2$ ps ($\theta_{rmb} = 1.6\,\mu$s), the MZI imbalanced delays $\delta T_{rma} = 510$ ps and $\delta T_{rmb} = 400$ ps, and the MZI static phases $\phi_{rma} = \pi/4$ and $\phi_{rmb} = \pi/8$.

3. Time delay concealment

We consider the case in which no message is transmitted ($d(t) = 0$) to show the role of the PRBS in the statistical properties of the carrier $x_{rma}(t)$. As commonly used in chaos communications cryptanalysis, the most robust methods to extract the time delay are the autocorrelation $C(s)$ and the delayed mutual information (DMI) between the value of the variable and its time-lagged version [5]. The graphs in Fig. 2 display the autocorrelation and the DMI computed from the transmitted phase proportional to $x_a(t)$, when no PRBS is used (Grey line, red on line) and with a PRBS at 3 Gb/s with an amplitude of $\pi/2$ (black line). In the first case both functions show peaks at $T = T_a + T_b$, $T + \delta T_a$, $T + \delta T_b$ and $T + \delta T_a + \delta T_b$, so that all relevant time delays can be readily identified. The delay time signature vanishes completely when the PRBS is included.

Figure 3 shows the size of peaks found in $C(s)$ and in the DMI at the relevant delay times as a function of the PRBS bit rate. The peaks are clearly distinguishable for zero bit rate (no PRBS added). When increasing the bit rate, the

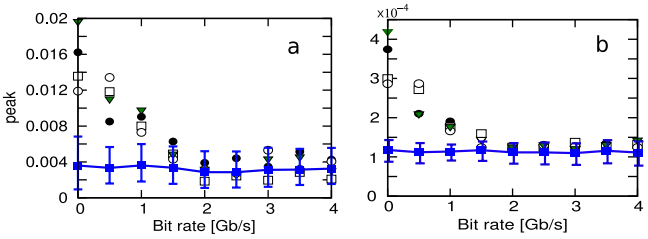

Figure 3: color on line. Absolute value of the peak (a): in $C(s)$, and (b):in the DMI, measured at T (•), $T + \delta T_b$ (□), $T + \delta T_a$ (○) and $T + \delta T_a + \delta T_b$ (∇), versus the PRBS bit rate. The horizontal line (blue on line) corresponds to the background mean value, while the bars stand for the deviation around this mean value. A series of length 267 times T was used.

peak size decreases and approaches the line (blue on line) corresponding to the background value of these functions. For low bit rates $p(t)$ and $p(t - \delta T_a)$ take the same value most of the time, so Δp_T vanishes most of the time and therefore the effect is small (see the concept of temporal non locality as introduced in [2]). 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. When the bit rate reaches a value corresponding to the inverse of δT_a (~ 1.97 Gb/s), Δp_T is typically non zero, and the PRBS plays a key role in the dynamics, concealing the time delay peaks.
One could notice the important following remark. While the PRBS key conceals the delay time in the chaotic carrier $x_a(t)$, we have numerically found that cross-correlation between $x_a(t)$ and $p(t)$ is of the order of 10^{-3}, meaning that the 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 PBRS is optimizing the mutual nonlinear mixing, resulting in an efficient mutual masking of each signal by the other.

At the receiver side (see [6] for more details on the receiver architecture), the decoding is performed as follows. The input phase modulated lightbeam is split into two paths. The long path is replicating the two serial processing chains used for the encoding at the emitter, in which of course a synchronized PRBS is involved, thanks to the knowledge of the digital secret key. The analog secret key is consisting in the hardware parameters determining the devices of the two serial processing chains, and their exact operating conditions. The output of the two processing chains, after being inverted, serves as the electrical input of PM'$_b$, which is intended to cancel the pseudo-random phase modulation superimposed to the message. The dynamics at the receiver is given by:

$$z_a + \tau'_a \frac{dz_a}{dt} + \frac{1}{\theta'_a} v_a = \beta'_a \cos^2\left[\Delta(w_b)_{T'_a} + \Delta p'_{T_a} + \phi'_a\right], \quad (3)$$

$$w_b + \tau'_b \frac{dw_b}{dt} + \frac{1}{\theta'_b} v_b = \beta'_b \cos^2\left[\Delta(x_a)T'_b + \Delta d_{T'_b} + \phi'_b\right], \quad (4)$$

where $dv_a/dt = z_a$, $dv_b/dt = w_b$, and primes refer to the receiver parameters. The output of PM'$_b$ 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 given by

$$P(t) \propto \cos^2\left[\Delta(x_a)_{T_m} + \Delta d_{T_m} - \Delta(z_a)T_m\right]. \quad (5)$$

For perfect synchronization, $z_a(t)$ is equal to $x_a(t)$, and $P(t)$ is corresponding to the message. If the receiver parameters are identical to the transmitter, the synchronization depends on the key. The differences $\delta_a(t) = z_a(t) - x_a(t)$ and $\delta_b(t) = w_b(t) - y_b(t)$ follow:

$$\delta_a + \tau_a \frac{d\delta_a}{dt} + \frac{1}{\theta_a}\varepsilon_a = -\beta \sin(\Delta\delta_{bT_a} + \Delta p'_{T_a} - \Delta p_{T_a}) \times \sin(2\Delta y_{T_a} + \Delta\delta_{bT_a} + \Delta p_{T_a} + \Delta p'_{T_a} + 2\phi_a) \quad (6)$$

$$\delta_b + \tau_b \frac{d\delta_b}{dt} + \frac{1}{\theta_b}\varepsilon_b = 0 \quad (7)$$

where $d\varepsilon_a/dt = \delta_a$ and $d\varepsilon_b/dt = \delta_b$. From Eq. (7) it turns out that δ_b decays to zero after a characteristic time

$$\frac{2\tau_b}{1 - \sqrt{1 - 4\tau_b/\theta_b}} \approx \theta_b \quad (8)$$

For $p'_{T_a} = p_{T_a}$, after δ_b has decayed to zero, the right hand side of Eq. (6) vanishes and therefore δ_a also decays to zero after a characteristic time

$$\frac{2\tau_a}{1 - \sqrt{1 - 4\tau_a/\theta_a}} \approx \theta_a, \quad (9)$$

Therefore the receiver synchronizes perfectly to the emitter after a transient time of the order $\theta_a + \theta_b$. However, if there is a mismatch in the PRBS then the right hand side of Eq. (6) does not vanish and therefore δ_a is finite, resulting in a degraded synchronization. Actually, for identical parameters, δ_b always decays to zero independently of any eventual key mismatch, indicating that the internal variable does synchronize. Synchronization degradation takes place on the transmitted variable.

4. Conclusion

In conclusion we have shown that a digital key can be integrated with a chaos-based communication system, in a way that on one hand it conceals the delay time, and on the other hand it is a necessary ingredient to decode the message. Besides bridging the gap between traditional cryptography and chaos-based encoding, the concealment of the time delay is particular 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. Finally, in a typical chaos-based communication systems as proposed in this article, the effective key-space of the encryption can be defined as the product of the analog key size, and the digital one. The scheme introduced here has a significantly larger key space, and furthermore it can be easily reconfigured to communicate between different systems. The proposed experimental approach might also be of interest for other purposes such as chaos based ultra-fast random number generation [7].

Acknowledgments

The reported results were mainly obtained at the issue of the European PICASSO project (FP6-2006-IST-2.5.1).

References

[1] A. Argyris et al., "Chaos-based communications at high bit rates using commercial fibre-optic links", *Nature* (London) Vol.438, 343, 2005.

[2] R. Lavrov, M. Peil, M. Jacquot, L. Larger, V. S. Udaltsov, and J. M. Dudley, "Electro–optic delay oscillator with non–local non linearity: optical phase dynamics, chaos, and synchronization," *Phys. Rev. E*, vol. 80, p. 026207, 2009.

[3] R. Lavrov, M. Jacquot, L. Larger, "Nonlocal nonlinear electro-optic phase dynamics demonstrating 10 Gb/s chaos communications", *IEEE J. Quantum Electron.*, Vol. 46, no.10, pp.1430–1435, 2010.

[4] 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", Journal of Lightwave Technology **28**, 2688 (2010).

[5] B. P. Bezruchko, A. S. Karavaev, V. I. Ponomarenko, and M. D. Prokhorov, "Reconstruction of time delay systems from chaotic time series", *Phys. Rev. E* Vol. 64, 056216 (2001).

[6] R. M. Nguimdo, P. Colet, L. Larger, and L. Pesquera, "Digital Key for Chaos Communication Performing Time Delay Concealment", *Phys. Rev. Lett.* Vol.107, 034103, 2011.

[7] A. Uchida et al., "Fast physical random bit generation with chaotic semiconductor lasers," *Nature Photon. (London)*, vol. 2, pp.728–732, 2008.