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

Time delay is well known as playing a key role in inducing strong chaotic behaviors, which are typically exploited for chaos communications. Unfortunately, this sensitive key parameter has also been found vulnerable when using standard time series identification techniques. Another limit of hardware cryptography relies on the fact that its parameter space dimension (a kind of equivalent to the digital key size in algorithmic encryption) is relatively low compared to software cryptography. To circumvent these drawbacks, we propose here to implement a currently suggested principle in algorithmic cryptography, which consists in mixing different algebra when constructing the encryption algorithm. In the context of secure chaos-based communications, a possible implementation of this idea would consist in combining a pseudo-random bit sequence (PRBS) typically used in standard 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. The proposed scheme is a double opto-electronic feedback system based on high speed phase chaos\(^1\), with constant intensity and an essentially featureless power spectrum. It allows on one hand to integrate a digital key required for decoding and on the other to conceal the delay time so that it cannot be identified from the time series using the typical methods. The emitter dynamics is given by the dimensionless variables \(x_1(t)\) and \(y_2(t)\)

\[
\begin{align*}
x_1 + \tau_1 \frac{dx_1}{dt} + \frac{1}{\theta_1} u_1 &= \beta_1 \cos^2(\Delta(x_1 + m)T_1 + \phi_1), \\
y_2 + \tau_2 \frac{dy_2}{dt} + \frac{1}{\theta_2} u_2 &= \beta_2 \cos^2(\Delta(x_1 + m)T_2 + \phi_2),
\end{align*}
\]

where \(du_1/dt = x_1, du_2/dt = y_2\) and \(\Delta(F)_m = F(t - t_0) - F(t - t_0 - \delta t_0)\). The parameters are the feedback strengths \(\beta_1 = \beta_2 = 5\), the delay times \(T_1 = 17\text{ns}\) and \(T_2 = 15\text{ns}\), the fast (slow) filter characteristic response times \(\tau_1 = 20\text{ ps} (\theta_1 = 1.6\text{ ns})\) and \(\tau_2 = 12.2\text{ ps} (\theta_2 = 1.6\text{ ns})\), the MZI imbalanced delays \(\delta T_1 = 510\text{ ps}\) and \(\delta T_2 = 400\text{ ps}\), and the MZI static phases \(\phi_1 = \pi/4\) and \(\phi_2 = \pi/8\). Figures. 1 b) and c) display DMI of the chaotic carrier as function of the delay without and with PRBS, respectively. It is seen that without PRBS, clear peaks appear at time-delays \(T, T + \delta T_1, T + \delta T_2\) and \(T + \delta T_1 + \delta T_2\). However, when PRBS is employed, time-delays cannot be identified anymore. Similar results were obtained from the computation of the autocorrelation function. Figures 1 d) and e) show the effects of mismatch \(\eta\) in the key by measuring the root-mean-square synchronization error \(\sigma\) and quality factor, respectively. Considering 10 Gb/s message with amplitude of \(\pi/2\) for Fig 1 e), it appears that even 4% of PRBS-mismatch is enough to considerably degrade the synchronization quality. Thus, we have shown that PRBS can be an efficient way to both provide further security and conceal the time delays in some electro-optic systems.