CHAOS 2009
2nd Chaotic Modeling and Simulation International Conference
June 1 - 5, 2009 Chania Crete Greece www.chaos2009.net

Breaking Chaotic Encryption using PDE's

A. Jacobo, M. C. Soriano, R. M. Nguimdo, P. Colet, C. Mirasso
Instituto de Fisica Interdisciplinar y Sistemas Complejos IFISC (CSIC-UIB), E-07122, Campus Universitat de les Illes Balears, Palma de Mallorca, Spain

Abstract: We show how, using the Ginzburg-Landau Equation, it is possible to decrypt a message encoded using Chaos Modulation. Then we introduce a new encoding method invulnerable to this attack.

In the context of chaotic communications using semiconductor lasers in many instances the message is codified such that the mean power of a bit 1 differs from that of bit 0. For example, in Chaos Modulation the transmitted signal is $P_t(t) = \left(1 - \varepsilon\, m(t)\right) P_m(t)$, where ε is the message modulation amplitude, $m(t)$ is the message being transmitted and $P_m(t)$ is the chaotic carrier.

We explore the possibility of using PDE's to filter the chaos and recover the message. In particular we consider the Ginzburg Landau Equation (GLE) in one dimension with an external forcing as a filter to find changes on the mean value and to recover the message:

$$\partial_t \psi(x) = d \cdot \partial_x^2 \psi(x) + \psi(x) - \psi(x)^3 + b \cdot h(x)$$

where ψ is the field, d is the diffusion constant and b is the forcing strength and $h(x)$ is the forcing, which here is directly related to the transmitted signal. Applying the GLE dynamics to $h(x)$ is possible to recover the encrypted message, as shown in Fig. 1.

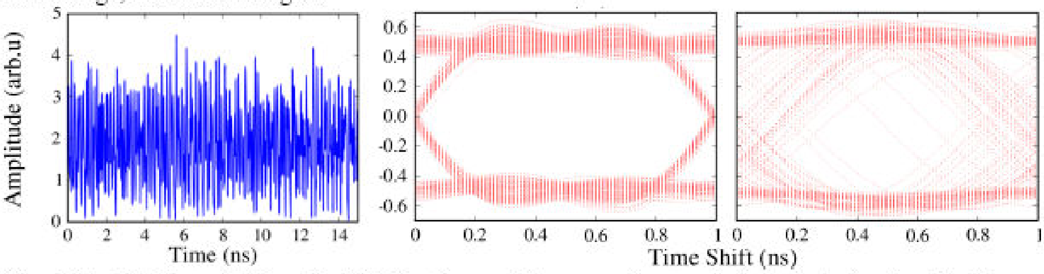

Fig. 1 From left to right: Transmitted signal (ε=0.04). Eye diagram of the recovered message by the authorized receiver. Eye diagram of the recovered message by the CGLE filter (d = 1; r = 0:65).

Despite that the eye diagram of the recovered message using the GLE is not as good as the eye diagram obtained by the authorized receiver, it still good enough to recover the message. The GLE method works because it is capable of detecting the changes on the mean value of the signal because of the presence of the bits '0' and '1'.

To improve the security, we propose a new encoding method, where the transmitted signal is formed according to the expression:

$$P_t(t) = \left(1 - \grave{o}\, m(t)\right) P_m(t) + \grave{o}\, m(t) \overline{P}_m,$$

where $\overline{P}_m$ is the mean of the chaotic carrier. The last term in this equation compensates for the changes in the mean value of the transmitted signal due to the message. The compensation term is chosen in such a way that $< P_t(t) >=< P_m(t) >= \overline{P}_m$ at any given time. In Fig. 2 we show how with this method the authorized receiver is able to recover the message, but the GLE filtering method completely fails to decode the message.

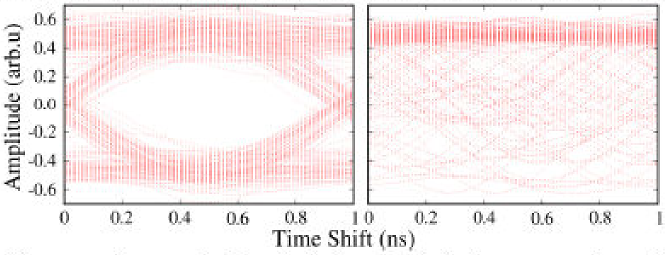

Fig. 2 Left: Eye diagram of the recovered message by the authorized received with the new encryption method. Right: Eye diagram of the message recovered by the GLE filter.

Finally, we also analyze the performance of an electro-optic encoding scheme against attacks performed with this method.