CHAOS-BASED COMMUNICATIONS USING SEMICONDUCTOR LASERS

Iana IVANCIUC, Alexandru PAVLOV

Technical University of Moldova

Abstract: *We report in this paper on the features of standard two-laser scheme in comparison with three-laser setup appropriate for chaos based communications. From our investigations, we learned that both, the two-laser and the three-laser systems are suitable to secure data exchange. However, the three-laser setup offers a better level of privacy because of its symmetry. We found out that three-laser setup has some specific advantages over the two-laser scheme in terms of digital security and privacy, however we mention that, due to its complexity, it is more difficult to implement.*

Keywords: *chaos, laser, cryptography, telecommunications, transmission, security;*

Chaos is a widely studied regime, which exhibits pseudorandom oscillations, strongly depending on starting conditions and parameter values. Nowadays, some of chaotic systems have been investigated and implemented in optics and telecommunication field. Among them, private communicational systems using chaotic waveforms [1] entirely are using the characteristic of chaos of being deterministic. Therefore, the approach to chaos secured data transmission consists in camouflaging a message into a complex noise-like waveform generated by a chaotic laser.

A relevant method of chaotic transmission consists of simply superposing chaos to the message at the transmitter. The composite signal is transmitted through the fiber link, and if the message is small enough, it is hidden both in the time and in the frequency domain. In sophisticated systems, it cannot be extracted, neither by filtering nor by using a correlator. Message recovery is performed by "master/slave" synchronization; at the receiver, a laser named "the slave" is used, having parameters very well matched with those of the transmitter laser named "the master" [2]. Therefore, the "slave" behaves as a nonlinear "chaos-pass," "message-stop," filter. The message can be reconstructed by making the difference between the received composite signal and the recovered chaotic waveform. The matching between the "master" and the "slave" must be high, if we want this system to work. After selecting a suitable pair of devices, this pair represent a hardware cryptographic key.

There are two ways of implementing chaos-protected communications, namely using two- or three-laser systems. Two-laser system have been described in [3]-[5]. Three-laser system consists of one "master" laser and two "slaves". "Master" injects the "slaves", one at the transmitter and one at the receiver. If the two "slaves" are "twins", they produce the same chaos and the message can be hidden at the transmitter and extracted at the receiver much as in the two-laser scheme. The main difference between these two transmissions is that in the three-laser scheme, both "slaves" are symmetrically injected by the third laser and by their external mirrors, while in the two-laser scheme, the "slave" is injected by its mirror and by the "master" and the "master" - by its own external mirror.

In conclusion, it is required to find out which system will be harder for an eavesdropper to infiltrate. On the one hand, for the two-laser scheme, the authorized sender and recipient have to select a laser with a proper mismatch. On the other hand, for the three-laser scheme, the twin pair can be usually found as close-proximity devices on the same wafer. Once the optimal pair has been selected, the eavesdropper is in a slightly better situation with the two-laser scheme: it has to find a laser similar to another one, without information about its parameters; however, one of these parameters does not need to be accurately matched. Nevertheless, it assumed that the eavesdropper cannot match the laser parameters by better than 5% and it is virtually impossible to extract the message in any case.

References:

1. A. Argyris, et al Nature 438. p.343. 2005.
2. V.Z. Tronciu, et al IEEE J. Quantum Electron. 46, p.1840-1846. 2010.
3. K. Ohtsubo Semiconductor Lasers: Stability, Instability and Chaos. New York: Springer; 2009.
4. S. Donati S, Mirasso C. IEEE Journal of Quantum Electronics. p. 1137-1196. 2002.
5. V. Annovazzi-Lodi, G. Aromataris *IEEE Journal of Quantum Electronics. p. 258-264. 2010.*