Security of chaos encryption in photonic integrated circuits

A. Bogris (1), A. Argiris (1), K.E. Chlonverakis (1) and D. Syvridis (1)
(1) Department of Informatics and Telecommunications, University of Athens, Ilisia, Athens, 157 84, Greece
Corresponding author e-mail: abogris@di.uoa.gr

Abstract: In this report we try to clarify significant issues regarding the security provided by telecommunication systems incorporating chaotic encryption.

1. Introduction
In this paper we try to explore theoretically the effect of codification method and the receiver’s architecture on the sensitivity of message extraction to parameter mismatch. Our perception is that FEC (Forward Error Correction) or other techniques cannot be omitted since security must be enhanced and investigated more thoroughly due to the analogue nature of our configuration. However, the concept of chaos synchronization is meaningful in the case where parameter mismatch is affecting significantly the message extraction. In that way, FEC or other techniques will more easily discriminate arbitrary receivers from matched ones. Our report studies the closed and open loop configurations in terms of baseband and subcarrier modulation [1] as a function of message amplitude considering significant parameter deviations.

2. Results and discussion
In real life situations the transmitter and receiver devices will not be perfectly matched to each other. Moreover, other parameters such as noise and transmission effects will further worsen the synchronisation between transmitter and receiver. In any case, this will lead to the requirement of higher message amplitudes for the achievement of the required SNR performance. Therefore it is helpful to calculate SNR of the decoded message in a noisy environment for both matched and deviating devices in open and closed loop configurations and for baseband and subcarrier modulation techniques [2]. Open loop is evidently less efficient for such low message amplitudes.
Utilizing subcarrier techniques, the message decoding efficiency is worse compared to the baseband scenario, expected due to the encryption of the message inside the most powerful part of the chaotic spectrum. The SNR difference between the matched and deviating devices is greater than 4dB and at low amplitudes reaches up to 8dB. This is an indication that deviating devices manifest less efficient synchronization at higher frequencies. Indicatively we report that for message amplitude equal to 22% and subcarrier frequency equal to 7GHz, the SNR for matched devices is 16dB while for unmatched devices is 9.5dB. Since SNR=10dB are large enough to provide BER less than $10^{-5}$ we observe (fig 1) that for modulation depth equal to 12% and subcarrier frequency 6.2GHz, the matched pair SNR is above threshold (12.2dB) while the slightly unmatched pair SNR is far below threshold (4.5dB, or BER>10^{-5}).

![SNR graph](image)

Fig 1 SNR of the decoded message for closed loop receiver as a function of message amplitude. Left: For chaos modulation, baseband and right: For chaos modulation, subcarrier.

3. Conclusions
Closed loop is the appropriate scheme in order to exploit the concept of chaos synchronization. The parameter mismatch affects the message extraction. As the mismatch increases, the amplitude of the message for which adequate SNR performance is achieved should be analogously increased. Additionally, subcarrier modulation technique has the ability to discriminate in a larger extend matched from deviating devices in terms of SNR performance of the decoded message compared to baseband modulation.

4. References