Romanian Reports in Physics **75**, 408 (2023)

OPTICAL CRYPTOGRAPHIC COMMUNICATIONS WITH NON-IDENTICAL CHAOTIC LASER SYSTEMS

I. R. ANDREI[1,*], S. SIMION[1], F. GAROI[1], M. BULINSKI[2], M. L. PASCU[1,2]

[1] National Institute for Lasers, Plasma, and Radiation Physics, 077125 Magurele/Bucharest
E-mails: *ionut.andrei@inflpr.ro*; *sandel.simion@inflpr.ro*;
florin.garoi@inflpr.ro; *mihai.pascu@inflpr.ro*
[2] University of Bucharest, Faculty of Physics, 077125 Magurele/Bucharest
E-mail: *mircea_bulinsky@yahoo.com*
[*] Corresponding author; e-mail: *ionut.andrei@inflpr.ro*

Received November 8, 2022

Abstract. We report secure data transmission performed using chaotic lasers with different external cavity geometries and applying the chaotic masking method based on subcarrier and phase modulations of the chaotic optical carrier. Two semiconductor lasers with similar multimode emission spectra and self-optical feedback provided, respectively, by ring and linear external cavities, were optically coupled and chaotically synchronized into a master – slave scheme. The transmitted message frequency modulates the radio frequency signal which modulates in phase the master chaotic carrier. Based on the robustness of the used encryption method and the synchronization characteristics of the two lasers, the decryption is conducted by the simple radio frequency spectrum monitoring of the slave emission.

Key words: chaotic semiconductor laser, chaos communication, phase modulation, chaos encryption.
DOI: https://doi.org/10.59277/RomRepPhys.2023.75.408

1. INTRODUCTION

The development of the field of data transmission involving electronic and computational technologies drove the development of data encryption systems [1]. In recent years, one area of secure transmission of optical information that has emerged is the encoding based on cryptographic systems (crypto-system) that use the chaotic properties of semiconductor laser emission [2–4]. With the development of this field the need to develop tools for evaluating and experimenting such systems has emerged [5, 6]. From this point of view, the external cavities semiconductor laser (ECSL) systems with chaotic dynamics are attractive for many applications [7], including optical communications [8, 9] and encoded data transmission [10–12], due to their main properties such as sensitive dependence on initial conditions, randomness and mixing and at the same time [4], broadband spectrum [13–15], synchronization [16] and the existence of different temporal scales [17].

Chaotic dynamics of two coupled chaotic laser systems become an integral part of crypto-systems due to their intrinsic property to be able to synchronize at the physical layer of the transmission system, which allows extremely fast modes of communication [12]. The enhancement of the encryption properties of chaotic signals, related to the increase of the encryption efficiency, is a purpose of the encryption systems. Chaos communications based on electro-optic modulation technique and feedback, have been studied and demonstrated as an alternative approach to electric or optic classical ones and have been successfully used in field experiments at comparable bit rates with optical intensity modulation [18, 19]. In the case of some modulation techniques, *i.e.* subcarrier (SM) and electro-optical phase (EOM) modulations, it was numerically and experimentally demonstrated [20–22] that the message can be very efficiently encrypted when the radio frequency carrier is within the frequency range where the chaos power density is maximized [20]. Also, the analyses on the decoding performance of subcarrier modulation technique, considering open-loop (solitary) and closed-loop (self-feedback) schemes at the receiver side, highlighted a robust operation in close-loop scheme and high sensitivity to parameter mismatch [20]. On the other hand, in the case of other communication schemes, good chaos synchronization and encoding performances were obtained for both open- and closed-loop cases [4, 23].

In this article, to the best of our knowledge, we report for the first time on the experimental results of data encryption and decryption by optical chaos, involving non-identical chaotic lasers. We start from two ECSLs with different closed-loop geometries, ring, and linear cavity, respectively, optically coupled, and dynamically synchronized into a master-slave configuration. Data encryption is done through an electro-optic phase modulator placed into the ring cavity which can modulate the master chaotic dynamics. The data decryption can be perform by direct RF spectrum analysis of the slave output [21], even if the two chaotic lasers are not identical, due to the efficiency of the approached encryption method, namely subcarrier frequency modulation (FM) of the radio frequency (RF) signal of electro-optic modulation of the chaotic carrier. This is possible due to the strong dependence of synchronization state on the relative phase between the master and slave external cavities; namely, a phase variation of the master substantially affects the correlation between the two laser outputs which induce an amplitude modulation [11]. Under special operating conditions, extracting the message directly from the slave dynamics was previously numerically and experimentally demonstrate on identical chaotic lasers [21].

The obtained results allow to better understand the mechanisms that contribute to data optical encryption and decryption based on chaos synchronization of two similar lasers, but with different origins of the chaos dynamics.

2. EXPERIMENTAL SETUP

The experimental set-up consists in a chaotically coupled laser system which was described in part elsewhere [23, 24] and was operated as it is shown therein. In addition to this coupled system, here, the master has a ring cavity and is unidirectionally coupled through an optical isolator with the slave (Fig. 1a). Lasers consist in two similar diode lasers (Mitsubishi ML101J8), both operated near the threshold laser at fixed parameters (injection current, temperature, and feedback power) so that they emit on the same laser active modes, distributed along 1 nm width spectral domain, in all modes of operation, solitary, self-feedback and coupled (Fig. 1b). The ECSLs working in low-frequency fluctuations chaotic regime are optically coupled through a NDF coupling attenuator (1% transmission) into a unidirectional lag synchronization scheme [23] at closed-loop laser powers of about 2 mW, and a time of fly between them of about 2 ns. Also, the two external cavities were matched in terms of external cavity oscillations frequencies at a difference of about 18 MHz, respectively, 354 and 336 MHz.

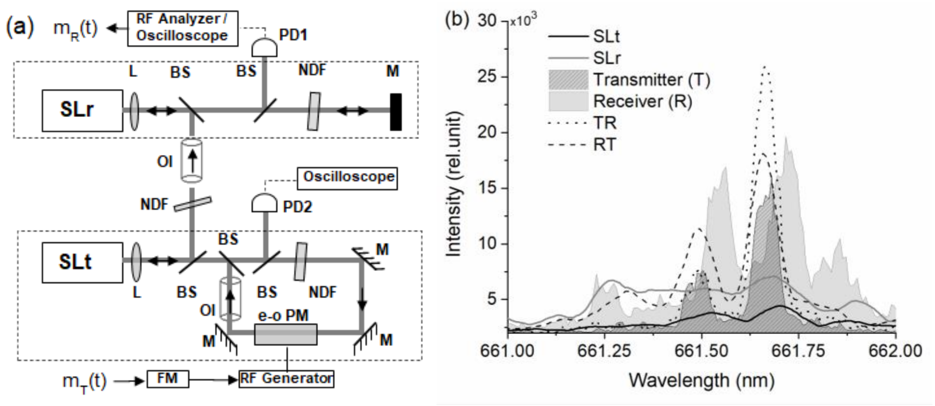

Fig. 1 – Chaotic laser system: a) transmitter-receiver coupling scheme; b) emission spectra for all modes of laser system operation, solitary (SLt, SLr), close-loop (T, R), and coupled (master-TR, slave-RT); SLt, SLr, transmitter and receiver lasers; L, collimation lens system; BS, beam splitter; NDF, neutral density filter; M, mirror; PD, amplified photodetector; OI, optical isolator; e-o PM, electro-optic phase modulator; FM, frequency modulation; RF, radio frequency modulation; $m_{\mathrm{T}}(t)$, and $m_{\mathrm{R}}(t)$, transmitted, and received, respectively, messages.

A Lithium Tantalate (LTA 360-80P, Conoptics Inc.) crystal type is included in the master cavity and is used as electro-optic phase modulator (e-o PM) to add the message (m_{T}). In the ring cavity, the radiation propagates unidirectionally through it determined by the specifications of the phase modulator (Fig. 1b). The message is inserted as a subcarrier frequency modulation of the RF sinusoidal signal of the e-o PM driving by using a signal generator with FM option incorporated (SG382, SRS Inc.). Transmitter and receiver signals were monitored using two amplified photodiodes PD1 and PD2 (ET-2030A, Laser 2000) of 0.5 ns rise time and 1.2 GHz bandwidth, and recorded by an oscilloscope (DPO7254, Tektronix) with 2.5 GHz bandwidth and maximum 40 GS/s sampling rate.

Transmission experiments were made by modulating the input voltage of the master LTA crystal, at about 80 MHz, modulated on its turn with messages of the order of 1 kHz. At the slave output, the carrier was directly monitored in real-time by a RF spectrum analyser (oscilloscope) to get the message (m_{R}).

3. RESULTS AND DISCUSSIONS

In this study, the chaotic masking method (CMS) was applied for secure data transmission, within which two modulation techniques are involved, subcarrier, and phase modulation of the chaotic carrier (both of sinusoidal form). The transmitted message of f_{FM} frequency modulates the RF carrier signal of f_0 frequency which modulates in phase ($\emptyset_f$) the master chaotic emission [21]:

$$\emptyset_f = \emptyset_0 + \emptyset_m \cos\left(2\pi[f_0 + \Delta f \cos(2\pi f_{FM} t)]t\right) ,$$

were $\emptyset_0$ is a constant phase.

Thus, the two standard modulation techniques (SM and EOM), which are independently used as encryption methods [20, 25], are combined for data encryption and transmission of the m_{T} message. The recovery of the m_{T} message is realized in certain specific conditions (MF and RF frequency domains) by simple RF spectra monitoring of the slave output using the photodetector and the oscilloscope [21]. This allows the recording of the m_{R} message present as a modulation of f_{FM} frequency of the RF signal.

In Fig. 2, the real-time master and slave power spectra associated to intensity time series are shown. For certain RF modulation frequencies, the master chaotic dynamics (optical signal noise) mask the electro-optical modulation signal in the phase of the laser radiation, in the sense that the modulation signal is not observed (recorded) in the master RF spectrum; RF modulation component is observed only in the slave spectrum (Fig. 2a). This indicates that a monitoring of the master signal by a third party, chaotically out of sync with it, does not lead to the detection of the frequency modulated RF signal. Instead, a receiver synchronized at the chaotic dynamics level with the master, detects the changes induced in the phase of the synchronization state (optical phase) between them. Thus, the f_{FM} frequency of the periodic oscillations induced in the master optical phase is present in slave power spectrum in the form of a maximum at the f_0 frequency modulated with the FM frequency (Fig. 2b).

The next analysis aimed to determine the working domains for RF and FM modulation frequencies and the amplitudes of the respective modulations. Due to the approached phase modulation technique and phase modulator type, the carrier signal must be sinusoidal with frequencies of 50 up to 250 MHz and amplitudes of maximum 600 mV. Investigating these ranges, it was observed that only a small number of frequencies and related amplitudes can be applied, so that the RF modulation signal is not identified in the master power spectrum. This is the first condition make possible the use of the encryption method (CSM).

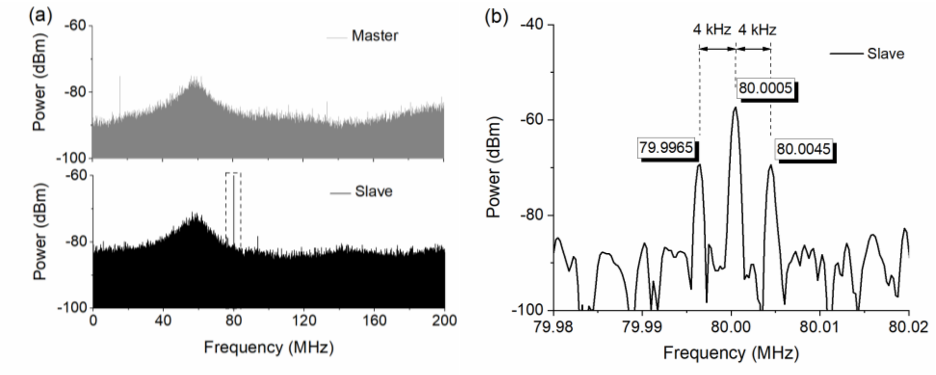

Fig. 2 – Experimental power spectra associated to intensity time series; a) RF master and slave spectra; b) detail of slave spectrum around the carrier frequency, which shows the f_{FM} frequency modulation of the RF carrier; f_0 = 80 MHz, f_{FM} = 4 kHz, amplitude of the f_{FM} signal, 270 mV.

In Fig. 3, the m_{R} recovered message of 4 kHz frequency can be viewed comparatively for two f_0 phase modulation frequencies, 70 and 80 MHz, and each at two amplitudes (u). The encrypted message present as a f_{FM} frequency modulation of 4 kHz is optimally detected for RF frequencies of the order of 80 MHz, as well at an amplitude of 270 mV. But, once the RF frequency changes to lower values, the quality of the recovered signal decreases. To values higher than 80 MHz, the RF signal becomes visible in the master power spectrum, in which case the encryption condition is not met.

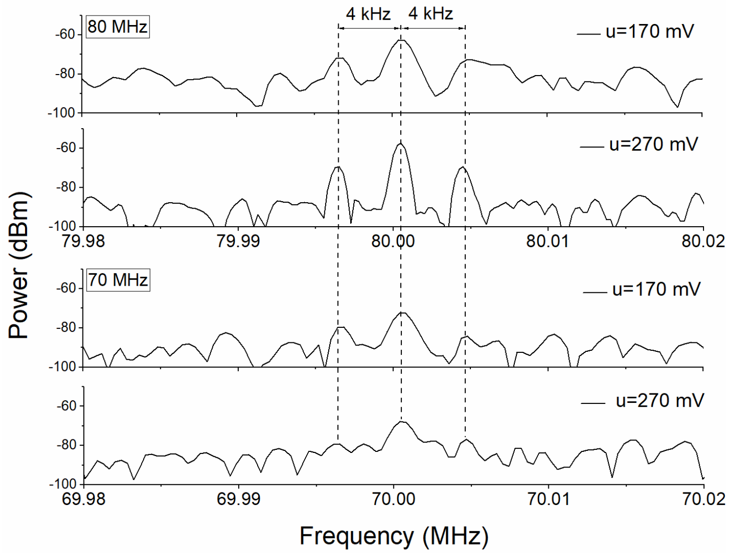

Fig. 3 – Power spectra: dependence of the m_{R} recovered signal on the phase modulation frequency and amplitude, for a subcarrier modulation of 4 kHz.

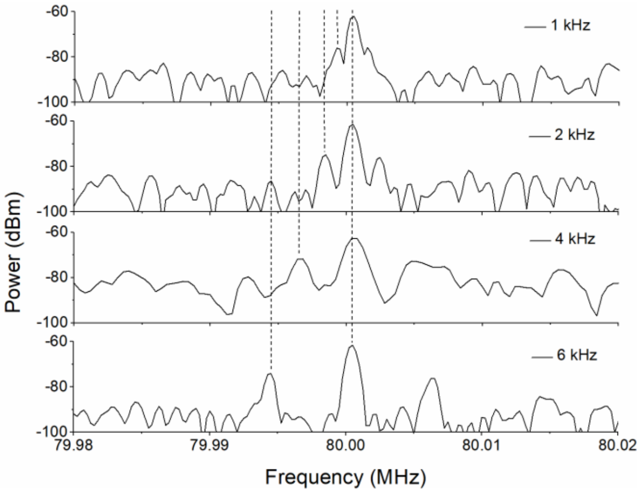

Fig. 4 – Power spectra: dependence of the m_R recovered signal on the subcarrier modulation frequency, for 80 MHz RF frequency and 170 mV amplitude.

Regarding the FM subcarrier modulation, the optimal frequencies are in a domain centred around 4 kHz for a RF modulation of 80 MHz at amplitudes around 200 mV. Figure 4 shows an analysis of the m_R recovered message quality, function of the subcarrier frequency. Among the analysed f_{FM} frequencies, the subcarrier modulation signals are also optimally detected for values between 1 and 6 kHz at a carrier frequency of 80 MHz and amplitudes of 170mV. This mean that, in a real case of data transmission, the message can be applied through the subcarrier modulation as a train of oscillations with different f_{FM} frequencies (0 and 1 pulse modulation) as is presented in Fig. 5. Here, a periodic pulse signal supplementally modulates the FM signal at a frequency of 600 Hz and mod deviation of 2 kHz. As it is the case in Fig. 5, by monitoring the value of the FM frequency it is possible to highlight the way to vary it, namely the pulsed modulation.

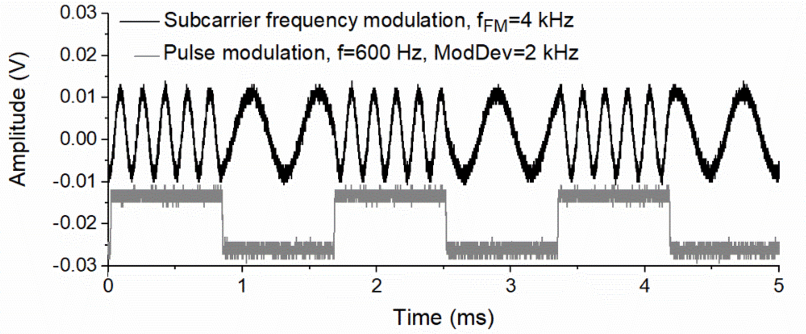

Fig. 5 – A sinusoidal signal of f_{FM} = 4 kHz pulse modulated at a frequency of 600 Hz with a mod deviation of 2 kHz.

As the results show, by applying the chaotic masking method based on subcarrier frequency and radio frequency modulations of master optical carrier, data decryption can be performed by RF spectrum analysis of the slave output, even if the optical transmission is established between two non-identical chaotic lasers.

4. CONCLUSIONS

In this work we demonstrated the possibility of encrypted data transmission between two chaotic systems that are not identical from the external cavity geometry point of view, namely ring and linear closed-loop cavities. Due to the robustness of the used encryption method and the similarity of the spectral characteristics of the two semiconductor lasers, the message could be decrypted by simply monitoring the RF spectrum of the slave system emission. The values of the involved frequencies were selected experimentally so that they ensure an efficient encryption and transmission of the message. At the same time, these values were also determined by the operating characteristics of the used equipment.

The results allow to understand the mechanisms that contribute to chaos optical data encryption based on optical and chaotic synchronization characteristics of two lasers and by applying subcarrier and phase modulation techniques.

Acknowledgements. This work was supported by grants of the Ministry of Research, Innovation and Digitization and CCCDI-UEFISCDI, projects number PN-III-P2-2.1-PED-2019-5283 and PN-III-P1-1.1-TE-2021-0949, and Nucleu Programme, ctr. No. 16N/08.02.2019.

REFERENCES

1. P. Singh and K. Kaur, *Database security using encryption*, 2015 International Conference on Futuristic Trends on Computational Analysis and Knowledge Management (ABLAZE), IEEE, 2015, pp. 353–358.
2. L. Kocarev and S. Lian, *Chaos-Based Cryptography: Theory, Algorithms and Applications*, Studies in Computational Intelligence **354**, Springer, Berlin, Heidelberg, 2011.
3. N. Holt, *Chaotic Cryptography: Applications of Chaos Theory to Cryptography*, 2017.
4. M. Sciamanna and K. A. Shore, *Physics and applications of laser diode chaos*, Nature Photonics **9**, 151–162 (2015).
5. J. S. Teh, M. Alawida, and Y. C. Sii, *Implementation and practical problems of chaos-based cryptography revisited*, Journal of Information Security and Applications **50**, 102421 (2020).
6. J. M. Amigó, L. Kocarev, and J. Szczepanski, *Theory and practice of chaotic cryptography*, Physics Letters A **366**, 211–216 (2007).
7. M. C. Soriano, J. García-Ojalvo, C. R. Mirasso, and I. Fischer, *Complex photonics: Dynamics and applications of delay-coupled semiconductors lasers*, Reviews of Modern Physics **85**, 421–470 (2013).
8. R. Vicente, C. R. Mirasso, and I. Fischer, *Simultaneous bidirectional message transmission in a chaos-based communication scheme*, Optics Letters **32**, 403 (2007).
9. A. Uchida, *Optical Communication with Chaotic Lasers: Applications of Nonlinear Dynamics and Synchronization*, 1st ed., Wiley, 2012.

10. A. Sanchez-Diaz, C. R. Mirasso, P. Colet, and P. Garcia-Fernandez, *Encoded Gbit/s digital communications with synchronized chaotic semiconductor lasers*, IEEE Journal of Quantum Electronics **35**, 292–297 (1999).
11. T. Heil, J. Mulet, I. Fischer, C. R. Mirasso, M. Peil, P. Colet, and W. Elsasser, *ON/OFF phase shift keying for chaos-encrypted communication using external-cavity semiconductor lasers*, IEEE Journal of Quantum Electronics **38**, 1162–1170 (2002).
12. S. Banerjee, L. Rondoni, and S. Mukhopadhyay, *Synchronization of time delayed semiconductor lasers and its applications in digital cryptography*, Optics Communications **284**, 4623–4634 (2011).
13. H. Someya, I. Oowada, H. Okumura, T. Kida, and A. Uchida, *Synchronization of bandwidth-enhanced chaos in semiconductor lasers with optical feedback and injection*, Optics Express **17**, 19536 (2009).
14. L. Zhang, B. Pan, G. Chen, L. Guo, D. Lu, L. Zhao, and W. Wang, *640-Gbit/s fast physical random number generation using a broadband chaotic semiconductor laser*, Scientific Reports **7** (2017).
15. A.-B. Wang, Y.-C. Wang, and J.-F. Wang, *Route to broadband chaos in a chaotic laser diode subject to optical injection*, Optics Letters **34**, 1144 (2009).
16. C. R. Mirasso, P. Colet, and P. Garcia-Fernandez, *Synchronization of chaotic semiconductor lasers: application to encoded communications*, IEEE Photonics Technology Letters **8**, 299–301 (1996).
17. I. Fischer, Y. Liu, and P. Davis, *Synchronization of chaotic semiconductor laser dynamics on subnanosecond time scales and its potential for chaos communication*, Phys. Rev. A **62**, 011801 (2000).
18. A. Argyris, D. Syvridis, L. Larger, V. Annovazzi-Lodi, P. Colet, I. Fischer, J. García-Ojalvo, C. R. Mirasso, L. Pesquera, and K. A. Shore, *Chaos-based communications at high bit rates using commercial fibre-optic links*, Nature **438**, 343–346 (2005).
19. R. Lavrov, M. Jacquot, and L. Larger, *Nonlocal Nonlinear Electro-Optic Phase Dynamics Demonstrating 10 Gb/s Chaos Communications*, IEEE Journal of Quantum Electronics **46**, 1430–1435 (2010).
20. A. Bogris, K. E. Chlouverakis, A. Argyris, and D. Syvridis, *Subcarrier modulation in all-optical chaotic communication systems*, Opt. Lett. **32**, 2134 (2007).
21. V. Annovazzi-Lodi, M. Benedetti, S. Merlo, T. Perez, P. Colet, and C. R. Mirasso, *Message Encryption by Phase Modulation of a Chaotic Optical Carrier*, IEEE Photon. Technol. Lett. **19**, 76–78 (2007).
22. V. Annovazzi-Lodi, G. Aromataris, and M. Benedetti, *Multi-User Private Transmission with Chaotic Lasers*, IEEE J. Quantum Electron. **48**, 1095–1101 (2012).
23. I. R. Andrei, G. V. Popescu, and M. L. Pascu, *Optical spectrum behaviour of a coupled laser system under chaotic synchronization conditions*, Journal of the European Optical Society: Rapid Publications **8**, 13054 (2013).
24. I. R. Andrei, C. Onea, P. E. Sterian, I. Ionita, and M. L. Pascu, *Control of slave chaotic dynamics by master current modulation in a chaotic coupled laser system*, Optoelectronics and Advanced Materials – Rapid Communications **13**, 284–289 (2019).
25. A. Argyris and D. Syvridis, *Chaos Applications in Optical Communications*, in Handbook of Information and Communication Security, P. Stavroulakis and M. Stamp, eds., Springer, Berlin, Heidelberg, 2010, pp. 479–510.