Eur. Phys. J. Special Topics **223**, 1441–1445 (2014)

DOI: 10.1140/epjst/e2014-02208-9

THE EUROPEAN PHYSICAL JOURNAL SPECIAL TOPICS

Editorial

Chaos and Cryptography: A new dimension in secure communications

Santo Banerjee[1,a] and J. Kurths[2,3,4,b]

[1] Institute for Mathematical Research, Universiti Putra Malaysia, Malaysia
[2] Humboldt University, Berlin, Germany
[3] Potsdam Institute for Climate Impact Research, Potsdam, Germany
[4] Institute for Complex Systems and Mathematical Biology, University of Aberdeen, Aberdeen, UK

Abstract. This issue is a collection of contributions on recent developments and achievements of cryptography and communications using chaos. The various contributions report important and promising results such as synchronization of networks and data transmissions; image cipher; optical and TDMA communications, quantum keys etc. Various experiments and applications such as FPGA, smartphone cipher, semiconductor lasers etc, are also included.

During the last two decades, chaos theory in the field of secure communication has attracted a lot of attention in various branches of Science and Engineering. To begin with, it appears as an application of chaos theory, apart from conventional cryptography [1]. Later, an application of chaos synchronization, motivated by the seminal work of Pecora and Caroll [2], opened a whole new dimension in cryptography [3–7].

Chaotic regimes can be observed in nature, in weather and climate, biology and ecological processes [8], economy and societies etc. The most important characteristic of chaos is to produce various complex patterns. The corresponding mathematical models can generate a large number of data, which are applicable as secret keys in the field of cryptography. Chaos theory has also the inherent property to connect it directly with cryptographic fundamental characteristics of "confusion" and "diffusion", which was reported in the earlier work by Shanon [9]. Additionally, chaotic systems have a deterministic yet unpredictable dynamics, which can be used as an effective tool in terms of a better cryptosystem.

In the beginning of secure communication using chaos theory, the approach was to use the pseudo random properties of the trajectories. Mainly basic models of discrete chaotic maps were used for crypto schemes. Chaos synchronization [10] has changed the approach of communication, it works as a whole cryptosystem. The driving system can be the transmitter and the response is the receiver. The simple idea was to mask a message with a chaotic signal and at the receiver end to decrypt it with the same synchronized signal [11].

[a] e-mail: santoban@gmail.com
[b] e-mail: Juergen.Kurths@pik-potsdam.de

Synchronization of coupled chaotic systems has become an integral part of cryptography. It allows effectively fast modes of communication as it works in the physical layer of the transmission system. Chaos based cryptography fully exploits the characteristics of chaotic dynamics, vs. determinism, ergodicity, sensitive dependence on initial conditions, randomness and mixing and at the same time, a strong dependence on any minimal variation of any parameter of the system. The need for secure data communication is even more necessary, given the ongoing rapidly increasing growth in telecommunications and internet.

The ways of modern communications are through internet, satellite, wireless, optical fibre, semiconductor devices etc. It is the utmost important to concerned about security issues over a communication network and confidentiality of data. As a result, a cryptographic protocol is required for every communication. The encryption method with chaos, was proposed by Baptista [12], which seems to be a much better encryption process than the previous ones. The phenomenon of chaotic synchronization generates a continuous feedback from sender to receiver. Various communication schemes based on synchronization, such as masking, shift keys, modulation etc. have been proposed [13]. Some interesting recent results such as adaptive synchronization with unknown parameters, modulating transmitted signals into the system parameters etc. have been also reported [14]. Those results are effective for secure communication.

Of late, synchronization of semiconductor lasers and its application in optical chaos based communication involving fiber lasers [15,16] and semiconductor lasers have been a potential area of research. These systems when subjected to optical feedback serve as an efficient alternate option for forming nonlinear transmitter and emitter systems which can be utilized in achieving high speed communication. A Chaotic regime is demonstrated in laser system subjected to chaotic oscillations by either injection from another source [17] or by reflection from an external mirror [18]. The complexity of decoding a message increases with the increase in the dimensionality of the system and with higher degrees of freedom of the chaotic carrier. This category of chaotic laser systems [19–21] upon synchronization has a potential for achieving enhanced security when they play the role of emitter and receiver systems which is realized by a high injection strength [22]. The inherent property of delay induced [23] nonlinear dynamics (due to the external cavities) will generate a chaotic carrier with considerable high dimensionality due to their highly chaotically fluctuating signals. This creates an additional layer of security to messages transmitted over fiber-optic networks together with achieving very high transmission rates. The corresponding models have multiple orbits, orbiting with high dimensionality, fast irregular pulsations, wave-length hopping, vast bandwidth ranging from a few giga-hertz to tens of giga-hertz, large correlation dimension of chaotic carrier [24–26], complexity and unpredictability of the chaotic carriers. The dynamics are resistant to linear filtering and frequency-domain analysis.

An experiment was conducted by Argyris et al. [27] which demonstrated the efficacy and potential of high speed optical communication when compared to other conventional modes of data transmission. As per as communication is concerned, a bi-directional transfer of information creates a flexibility in attaining the role of transmitter and receiver during communication. The simultaneous transmission of information with bi-directional coupling has motivated to investigate synchronization phenomena of a mutually coupled chaotic semiconductor laser system. The most useful theoretical model of a SL laser is the Lang-Kobayashi (L-K) delay-differential rate equations (DDE) [28]. The system operates in a single longitudinal mode thereby acting as a transceiver. The synchronization based continuous time cryptosystem produces a symmetric cryptography using optical feedback. Further more, the receiver also operates with the identical feedback mechanism through an external

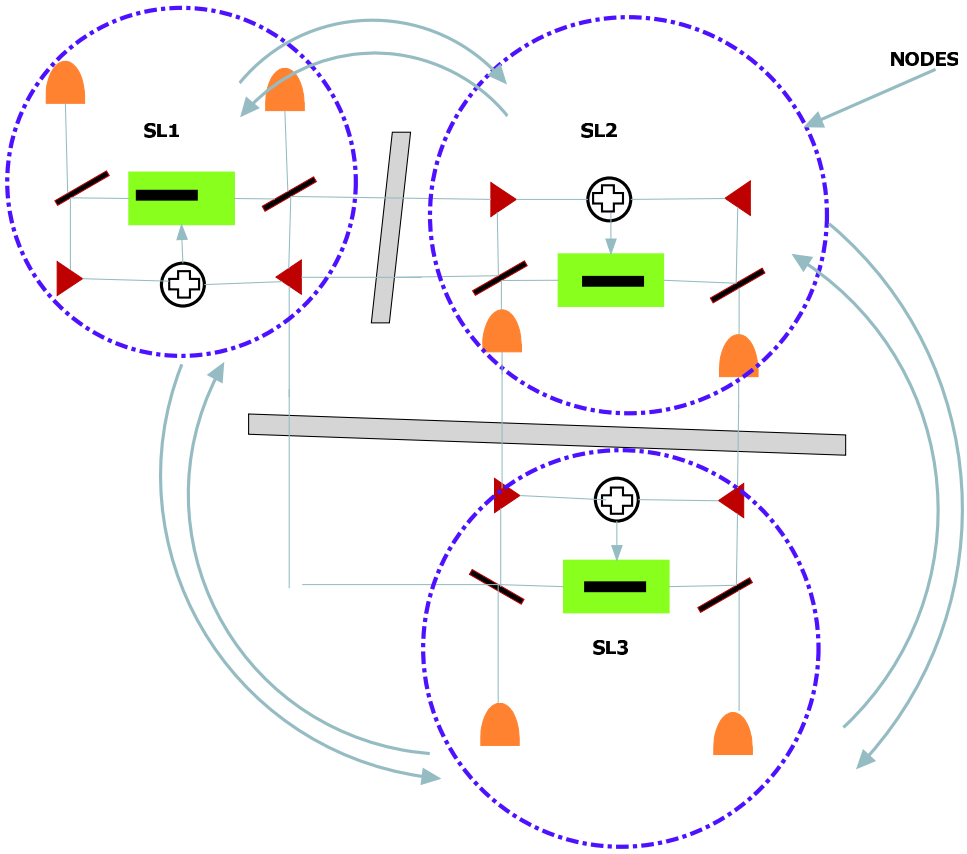

Fig. 1. The schematic ring diagram of three semiconductor lasers.

mirror. Therefore, this arrangement forms a closed-loop system which has been proved to render strong security even when the closed loop system has a longer synchronization time and is less robust against frequency detuning and it is more popular than often used open loop schemes.

Recent research on synchronized SLs has examined to design optical communication networks [29]. To reveal dynamical properties of optical networks, it is very important to understand the features of basic topology, such as rings or star. Figure 1 shows a schematic diagram of three synchronized SLs with bi-directional coupling. The synchronization is robust in both star and ring topology with n-number of distinct nodes. Moreover, the output power also increases with an increasing number nodes inside the network.

This special issue on "Chaos, Cryptography and Communications", consists of 22 original regular research articles. Each contribution refers to recent developments of cryptography and communication theory using chaos. Several theoretical and experimental results are presented here. The articles can be grouped into three categories, namely 1. "Synchronization of systems and networks for communication" [30–41]; 2. "Chaos based image encryption, stream cipher and authentication" [42–48] and 3. "Other applications for communication" [49–51]. In [30] the authors presented a numerical analysis on isochronal synchronization between chaotic oscillators and applied it in TDMA to network communication. The security,limitations and potentials of the proposed scheme are also well investigated.

In [31], the synchronization between two time delayed systems was established with numerical simulations and FPGA experiments. The results are very useful for communication and cryptographic encoding.

In [32], a communication scheme is introduced with synchronization between LPV discrete systems. These results are well established with analytical and numerical support.

Articles by [33] and [41] are on synchronization between fractional order systems. The results are novel and well applicable for cryptographic encoding.

In [34], a new synchronization scheme for networks is established via numerical and analytical support. In [35,36,40] synchronization between ODE's and various control techniques are studied.

In [39], phase synchronization is established between a pair of nonlinear data sets. A link for communication is also reported.

In [42–45,47,48] various cryptographic scheme is reported for streamcipher and image encryption. The image processing and crypto-analysis of few existing schemes are also investigated. A biometric authentication based on a fractal analysis is given in [46].

Other applications with Laser, noise and quantum keys are presented in [49–51] respectively. The results are well established with simulations and analytical justifications.

We would like to thank the authors for their contributions and the referees for their efforts in reviewing the manuscripts. We hope this issue will be helpful for the scientists and researchers working on the field of communication and cryptography.

Finally, we would like to thank all members of EPJ ST, for hosting this special issue, specially Dr. Caron, Sabine Lehr and Isabelle Houlbert for their kind support.

References

1. E. Ott, *Chaos in Dynamical Systems* (Cambridge University Page, Cambridge, 2002)
2. L.M. Pecora, T.L. Carroll, Phys. Rev. Lett. **64**, 821 (1990)
3. R. Matthew, Cryptologia **8**(1), 29 (1984)
4. L. Kocarev, G. Jakimoski, T. Stojanovski, I. Parlitz, Proc. IEEE Int. Symposium Circ. Syst. **4**, 514 (1998)
5. L. Kocarev, IEEE Circ. Syst. Mag. **1**(3), 6 (2001)
6. S. Mukhopadhyay, M. Mitra, S. Banerjee, edited by S. Banerjee, Chaos Synchronization and Cryptography for Secure Communications: Applications for Encryption (IGI Global Publishers, USA, 2010), ISBN: 1615207376, p. 476
7. S. Banerjee, D. Ghosh, A. Ray, A.R. Chowdhury, Europhys. Lett. **81**, 20006 (2008)
8. S. Banerjee, A.P. Misra, L. Rondoni, Physica A **391**, 107 (2012)
9. C. Shannon, Bell Syst. Techn. J. **28**(4), 656715 (1949)
10. A. Pikovsky, M. Rosenblum, J. Kurths, *Synchronization: An Universal Concept in Nonlinear Sciences* (Cambridge University Press, Cambridge, 2001)
11. L. Kocarev, K.S. Halle, K. Eckert, L.O. Chua, U. Parlitz, Int. J. Bifurc. Chaos **2**, 709 (1992)
12. M.S. Baptista Phys. Lett. A **240**(1), 50 (1998)
13. K.M. Cuomo, A.V. Oppenheim, Phys. Rev. Lett. **71**, 65 (1993)
14. X. Wu, Chaos **16**, 043118 (2006)
15. E.A. Rogers-Dakin, J.G. Ojalvo, D.J. De Shazer, R. Roy, Phys. Rev. E **73**, 045201 (2006)
16. G.D. Van Wiggeren, R. Roy, Science **5354**, 1198 (1998)
17. V.A. Lodi, S. Donati, M. Manna, IEEE J. Quant. Electron **30**, 1537 (1994)
18. J. Mork, B. Tromborg, J. Mark, IEEE J. Quant. Electron **28**, 93 (1992)
19. J.K. White, J.V. Moloney, Phys. Rev. A **59**(3), 2422 (1999)

20. P. Saha, S. Banerjee, A.R. Chowdhury, Chaos, Solitons Fractals **14**(7), 1083 (2002)
21. S. Banerjee, P. Saha, A.R. Chowdhury, Phys. Lett. A **291**(2), 103 (2001)
22. A. Murakami, Phys. Rev. E **65**(5), 056617 (2002)
23. K. Ikeda, K. Matsumoto, Physica D **29**, 223 (1987)
24. Y. Takiguchi, K. Ohyagi, J. Ohtsubo, Opt. Lett. **28**(5), 319 (2003)
25. A. Wang, Y. Wang, H. He, IEEE Photonics Technol. Lett. **20**(19), 1633 (2008)
26. D.M. Kane, J.P. Toomey, M.W. Lee, K.A. Shore, Opt. Lett. **31**(1), 20 (2006)
27. A. Argyris, et al., Nature **7066**, 343 (2005)
28. R. Lang, K. Kobayashi, IEEE J. Quant. Electr. **16**, 347 (1980)
29. J. Zamora Munt, C. Masoller, J. Garcia Ojalvo, R. Roy, Phys. Rev. Lett. **105**, 264101 (2010)
30. J.M.V. Grzybowski, E.E.N. Macau, T. Yoneyama, Eur. Phys. J. Special Topics **223**(8), 1447 (2014)
31. D. Valli, B. Muthuswamy, S. Banerjee, M.R.K. Ariffin, A.W.A. Wahab, K. Ganesan, C.K. Subramaniam, J. Kurths, Eur. Phys. J. Special Topics **223**(8), 1465 (2014)
32. M. Halimi, G. Millérioux, Eur. Phys. J. Special Topics **223**(8), 1481 (2014)
33. S. Bhalekar, Eur. Phys. J. Special Topics **223**(8), 1495 (2014)
34. A. Ray, A. Roychowdhury Eur. Phys. J. Special Topics **223**(8), 1509 (2014)
35. S. Vaidyanathan, Eur. Phys. J. Special Topics **223**(8), 1519 (2014)
36. P. Rani Sharma, A. Singh, A. Prasad, M. Dev Shrimali, Eur. Phys. J. Special Topics **223**(8), 1531 (2014)
37. R. Aguilar-López, R. Martínez-Guerra, C.A. Perez-Pinacho, Eur. Phys. J. Special Topics **223**(8), 1541 (2014)
38. A.K. Mittal, A. Dwivedi, S. Dwivedi, Eur. Phys. J. Special Topics **223**(8), 1549 (2014)
39. S. Mukherjee, S. Kumar Palit, S. Banerjee, M.R.K. Ariffin, D.K. Bhattacharya, Eur. Phys. J. Special Topics **223**(8), 1561 (2014)
40. K. Kemih, M. Halimi, M. Ghanes, H. Fanit, H. Salit, Eur. Phys. J. Special Topics **223**(8), 1579 (2014)
41. Y. Wang, K. Sun, S. He, H. Wang, Eur. Phys. J. Special Topics **223**(8), 1591 (2014)
42. G. Vidal, M.S. Baptista, H. Mancini, Eur. Phys. J. Special Topics **223**(8), 1601 (2014)
43. K. Ganesan, K. Murali, Eur. Phys. J. Special Topics **223**(8), 1611 (2014)
44. P. Shanmugavadivu, P.S. Eliahim Jeevaraj, Eur. Phys. J. Special Topics **223**(8), 1623 (2014)
45. T.M. Hoang, D. Tran, Eur. Phys. J. Special Topics **223**(8), 1635 (2014)
46. N.M.G. Al-Saidi, M.R.M. Said, Eur. Phys. J. Special Topics **223**(8), 1647 (2014)
47. H.T. Panduranga, S.K. Naveen Kumar, Kiran, Eur. Phys. J. Special Topics **223**(8), 1663 (2014)
48. L. Hao, L. Min, Eur. Phys. J. Special Topics **223**(8), 1679 (2014)
49. D.S. Goldobin, Eur. Phys. J. Special Topics **223**(8), 1699 (2014)
50. A.F. Metwaly, M.Z. Rashad, F.A. Omara, A.A. Megahed, Eur. Phys. J. Special Topics **223**(8), 1711 (2014)
51. R. Meucci, K. Al Naimee, M. Ciszak, S. De Nicola, S.F. Abdalah, F.T. Arecchi, Eur. Phys. J. Special Topics **223**(8), 1729 (2014)