Introduction to the Feature Section on Optical Chaos and Applications to Cryptography

WE ARE currently immersed in a society in which information transmission plays a crucial role, and where an ever-growing capacity for communications services is required. Two of the major issues in communications are privacy and security. Traditionally, public key cryptosystems based on software techniques have covered these two issues, although the security relies on computational complexity theory and they are, consequently, insecure according to Shannon information theory. These systems can use a rather short secret parameter, known as the key, or they can encode the message directly. It is especially suitable for exchanging private information on a large network of subscribers, where everyone can send and receive messages to and from anyone. Its level of security has been kept high by increasing the key length (256–512 bits) as the performance of computers increases, to prevent brute force attacks. Its principal drawback is that it requires some means (or institution) to validate the keys. Otherwise, if an eavesdropper E (Eve) can intercept a communication between subscribers A (Alice) and B (Bob), she could convince both to use her own key instead of the correct ones. A and B would then transmit to each other in a completely transparent manner to E.

Recently, quantum cryptography has been proposed as an alternative to software encryption. Despite its potential, its applicability is still very far from being proven. The objective of "Quantum Cryptography"—also termed "Quantum Key Distribution" (QKD)—is to exploit the properties of quantum optics in order to secretly share a random bit sequence between two users. Once the key has been exchanged, the two parties can communicate, by conventional means, a message over a public channel by encrypting with the key a message of equal length. This scheme belongs to the class of hardware-key cryptography and can be used only to exchange a secret key. It is not suitable for a whole message. In QKD schemes, security is guaranteed by the fundamental laws of quantum mechanics, and therefore is extremely high. The key is sent over a quantum channel. If an eavesdropper taps the line, transmission errors occur due to the quantum-mechanical nature of photons. To detect these errors, the legitimate users verify statistically a set of shared bits. If errors are detected in the verification process, the users conclude that the line is attacked.

An alternative and simple way to improve the security of an encrypted message can be realized by additionally encoding at the physical layer using chaotic carriers generated by components operating in the nonlinear regime. Semiconductor lasers are ideal candidates for the realization of these nonlinear emitter and receiver systems. They are already inherently nonlinear devices that, under various operating conditions, exhibit nonlinear dynamical behavior associated with, e.g., fast irregular pulsations of the optical power or wavelength hopping.

The essence of optical communication using chaotic carriers resides in the fact that two spatially separated chaotic lasers can synchronize to each other; "synchronization" means that the irregular time evolution of the emitter laser, either in the optical power or the wavelength, can be well reproduced by the receiver laser.

Once the two lasers are synchronized, the chaotic output of the emitter laser can be used as the carrier on which the key or, in general, the message is encoded. The other laser, in the receiver system, allows the message to be extracted. Decoding is based on the nonlinear phenomenon of chaos synchronization between emitter and receiver. The key issue resides in the fact that the receiver synchronizes to the chaotic oscillations of the emitter (the carrier), while suppressing the encoded message. Therefore, by comparing the input (carrier+message) and output (carrier only) of the receiver, the message can be extracted.

The key for effective synchronization (and, thus, for decoding) lies in the use of similar components for both chaotic systems, with close matching with respect to parameters and operation conditions. Parameter mismatch is a key issue for synchronization. The process of decoding without the right receiver is difficult to achieve due to the high frequencies involved and the large number of degrees of freedom of the chaotic carrier. It is worth noting that chaotic carriers provide, in semiconductor diode lasers, a broad spectrum (typically in the 10–100-GHz range) in which the message is hidden. Although the maximum rate at which a message can be encoded has not yet been determined, preliminary studies suggest that its bandwidth must be smaller than the carrier's bandwidth. The properties of these carrier signals, and the way the message is encoded, are such that with a linear filtering process it is not possible to extract the message. Also, correlators and frequency-domain analysis would fail. It is important to note that this technique could very well complement the already existing methods of encryption, namely, software encryption. The innovation resides in the fact that encryption is reinforced by codifying at the hardware level.

Chaotic signals have similar features to those used in broad spectrum communications and related fields where information is hidden within complex codes or noisy signals. Up to the present, the methods for generating chaotic signals have generally used relatively simple electrical circuits. There have been two main problems with this approach. First, most of the circuits have been designed in the audio range with message bandwidths limited to some tens of kilohertz. Although RF circuits may be contemplated, it is difficult to attain the multi-gigahertz frequencies required in many communication channels. Furthermore, most already installed, high-speed communication networks are based on optical fibers. Therefore, a codification scheme based directly on an optical carrier is highly desirable. Second (and more fundamental), the chaotic carrier generated electronically is, in general, low-dimensional, which results in a low level of confidentiality when applied

Publisher Item Identifier 10.1109/JQE.2002.801951.

to secure communication transmissions. Both of these issues are overcome by the proposed use of high-dimensional chaos generated by semiconductor lasers. Recently, theoretical and experimental results have shown the feasibility of synchronizing the so-called hyper-chaos in all-optical and electro-optical systems. Although the previously mentioned experiments have succeeded on a laboratory level, the feasibility of achieving secure communications in real world communication networks using chaotic synchronized lasers has yet to be proven.

In this Feature Section, we have six contributions from pioneering groups working on optical chaos synchronization and encryption. The different contributing groups are located in Europe, the U.S., and Japan, indicating the potential technological interest of this technique to improve privacy in the transmission of secure data. As already mentioned, the two more widely used techniques to make a semiconductor laser operate in a chaotic regime are optical and electrooptical feedback. Both techniques are well represented in this feature issue. Theoretical, numerical and experimental results are presented. The first four papers deal with optical feedback. J. Ohtsubo studies, both theoretically and experimentally, the synchronization properties of chaotic semiconductor lasers, subject to optical feedback, and the application to chaotic data encryption. He carefully discusses the two possible schemes for chaos synchronization, namely complete and generalized, and the robustness of the synchronization is studied with respect to parameter mismatches. He also demonstrates message transmission of sinusoidal signals at 1.5 GHz. S. Sivaprakasam *et al.* experimentally investigate two chaotic semiconductor lasers, also with optical feedback. They study both unidirectional and bidirectional coupling and find experimental conditions for synchronization and anti-synchronization, and a regime of anticipated synchronization. T. Heil and coworkers study the synchronization properties of two external cavity semiconductor lasers that are unidirectionally coupled and whose external cavities can be slightly different. They find that synchronization is optimum when both cavities are exactly equal, but that synchronization can be lost when the cavities differ to within subwavelength precision. Based on this fact, they propose and numerically demonstrate a novel technique to encode bits by using feedback-phase variations. V. Annovazzi-Lodi *et al.* consider a semiconductor laser subject to optical feedback from a mirror located at the end of a long fiber cavity. They focus on the analysis of the chaotic regime as a function of the pump current, back reflection level, and cavity length in a configuration which would be appropriate for integrated optical circuits. They compare experiments with numerical simulations of the rate equation model. The two other papers concentrate on electro-optical feedback. Although at first glance they look similar, the two proposed techniques are quite different. J. P. Goedgebuer and coworkers use semiconductor lasers with nonlinear electro-optical feedback. The core of the chaotic transmitter and receiver is formed by an electro-optical modulator with strong nonlinearities that generates extremely high-dimensional waveforms in which a message can be encoded. On the other hand, J.-M. Liu and coworkers use linear conversion from light to current, yielding a linear external electro-optical feedback. Based on this configuration, they numerically study the performance of the system when codifying with different techniques, such as chaos masking, additive chaos modulation or chaos shift keying, at a bit rate of 10 Gb/s. We believe that these contributions will encourage other researchers to study and develop new possibilities for this emerging field of optical chaos encryption.

SILVANO DONATI, *Guest Editor*
University of Pavia
Department of Electronics
27100 Pavia, Italy

CLAUDIO R. MIRASSO, *Guest Editor*
Universitat de les Illes Balears
Departament de Fisica
E-07071 Palma de Mallorca, Spain

Silvano Donati (M'75–SM'98) received the Laurea degree (cum laude) in physics from the University of Milan, Milan, Italy, in 1966.

He has been with the University of Pavia, Pavia, Italy, since 1975. He was a Lecturer in electronics circuits, electronic materials and technologies, and electro-optic systems before becoming a Full Professor of optoelectronics in 1980 with the Department of Electronics. He has carried out research on electrooptical instrumentation (laser interferometry, fiber gyros, fiber-optic current sensors), all-fiber components for communications, and more recently noise in devices, coupled oscillators, and optical chaos. He was previously with Centro Informazioni Studie d'Experiweenze (CISE), Milan, Italy, working on photodetectors and laser instrumentation. He has authored or coauthored one book, *Photodetectors*, (Englewood Cliffs, NJ: Prentice-Hall, 1999), and approximately 200 papers, and holds ten patents.

Dr. Donati has been Guest Editor of the *IoP Journal of Optics* issue on Interferometry (June 1998), the IEEE JOURNAL OF SELECTED TOPICS IN QUANTUM ELECTRONICS issue on Fiber Optics Passive Components (September 1999), and the SPIE *Optical Engineering* issue on Optical Distance Measurements (January 2001). He was the Editor of *Alta Frequenza* (1986–1992), a review in electronics published by the the Associazio Elettrotecnica Italiana (AEI). He has organized several national and international meetings, in which his roles include Chairman of Fotonica (1997) and Elettroottica (1994) with AEI, WFOPC (1998), ODIMAP II (1999), WFOPC II (2000), and ODIMAP III (2001). In 1997, he founded the LEOS Italian Chapter, for which he Chaired until 2001. He is now the LEOS Vice President for Membership in Region 8. He and his research group have been awarded six prizes, including the Marconi Gold Medal (1999) for a scientific career. He is an Emeritus Member of AEI, and a member of OSA, SPIE, and IMAPS.

Claudio R. Mirasso was born in Buenos Aires, Argentina, in 1960. He received the M.Sc. and Ph.D. degrees in physics from the Universidad Nacional de La Plata, La Plata, Argentina, in 1984 and 1989, respectively.

He was a post-doctoral Researcher in the Physics Department, Universitat de les Illes Balears, Palma de Mallorca, Spain (1990–1992), a Visiting Professor at the Modern Physics Department, Universidad de Cantabria, Cantabria, Spain, and the Physics Department, Universitat de les Illes Balears (1992–1994), respectively, and a Scientific Researcher of the Consejo Superior de Invesitgaciones Cientificas, Madrid, Spain, and a European post-doctoral Researcher at the Physics Department, Free University, Amsterdam, The Netherlands (1994–1995). Since 1996, he has been an Associate Professor with the Physics Department, Universitat de les Illes Balears. He is currently also Coordinator of the European project Optical Chaos Communication Using Laser Diode Transmitters (OCCULT). He has authored or co-authored over 100 publications, including about 60 journal papers. His research interests include instabilities in semiconductor lasers, synchronization and control of chaotic semiconductor lasers, vertical-cavity semiconductor lasers, and applications of nonlinear dynamics.