Chapter 13

Private Communications Using Optical Chaos

Valerio Annovazzi-Lodi, Giuseppe Aromataris and Mauro Benedetti

Additional information is available at the end of the chapter

http://dx.doi.org/10.5772/intechopen.70896

Abstract

After a brief summary of the basic methods for secure transmission using optical chaos, we report on most recent achievements, namely, on the comparison between the standard two-laser and the three-laser schemes and on the network architecture for multiuser secure transmission. From our investigations, we found that while both the basic two-laser and the three-laser schemes are suitable to secure data exchange, the three-laser scheme offers a better level of privacy due to its symmetrical topology. Moreover, while transmission based on optical chaos is usually restricted to point-to-point interconnections, a more advanced solution, derived from the well-known public key cryptography, allows for private message transmission between any couple of subscribers in a network.

Keywords: chaos, cryptography, steganography, laser, telecommunications, synchronization

1. Introduction

Chaos [1] is a widely studied regime of many nonlinear systems, which exhibit pseudorandom oscillations, strongly depending on starting conditions and parameter values. Several chaotic systems have been investigated and implemented in optics [2, 3]. For example, a semiconductor laser may be routed to chaos by injection from another source or simply by reflection or diffusion from an external optical element. In the last years, several chaos applications have been proposed in the telecommunication field. Among them, private communication using chaotic waveforms fully exploits the characteristic of chaos of being deterministic, exhibiting, however, a strong dependence on even minimal variations of the system parameters.

The basic approach to chaos secured data transmission consists in hiding or coding a message into the very complex noise-like waveform generated by a chaotic laser [4, 5].

In most schemes, chaos generation is based on delayed optical feedback, that is, on reflection of a fraction of the laser emission back into its cavity by an external mirror or even from the tip of the output fiber [4–7]. With this approach, we can select different chaos characteristics, such as amplitude and bandwidth, by acting on the mirror or fiber position. Using standard distributed feedback laser (DFB) telecommunication lasers, complex and robust chaotic waveforms can be generated, which modulate the laser on a large bandwidth, well in excess of its relaxation frequency.

A suitable method of chaotic transmission consists of simply superposing chaos to the message at the transmitter (Tx), in order to strongly reduce its signal-to-noise ratio (SNR). The composite signal is transmitted through the fiber link, and if the message is small enough, it is efficiently hidden both in the time and in the frequency domain. In well-designed systems, it cannot be extracted, neither by filtering nor by using a correlator.

In most cases, message recovery is performed by master/slave synchronization; at the receiver (Rx), another laser (the slave, SL) is used, having parameters very well matched with those of the transmitter laser (the master, MS). The waveform from the optical link (chaos + message) is injected into the slave. Under proper operating conditions, the slave laser is forced to synchronize to the chaos of the MS (i.e., the two devices generate almost exactly the same chaotic waveform), without, however, synchronizing the message. In other words, the SL behaves as a nonlinear "chaos-pass," "message-stop," filter. Thus, the message can be extracted by making the difference between the received composite signal and the recovered chaotic waveform.

The degree of matching required between master and slave for efficient synchronization is significantly high. A suitable pair of devices ("twins") must be selected in close proximity from the same wafer. This laser pair represents the (hardware) cryptographic key. Chaos cryptography is compatible, and can be superposed, to standard algorithmic cryptography.

2. Chaos-protected transmission schemes

In **Figure 1**, we show a typical implementation of the chaos transmission scheme, which is usually referred to as chaos masking (CM), since the message is added to the chaotic waveform, usually by an external amplitude modulator. Other schemes are possible [4, 5], which are broadly referred to as "chaotic cryptography" in the literature, even though in most cases, such as in **Figure 1**, the term "chaotic steganography" would better describe these methods. For example, in chaos shift keying (CSK), the message directly modulates the pump current of the transmitter laser, and in additive chaos masking (ACM), the message is applied by using a third laser modulated in amplitude by the analog or digital message, whose output is then combined with the chaotic waveform.

A large experimental and numerical work has been performed on such topic by different authors. Numerical analysis is usually based on the Lang-Kobayashi (L-K) model [8], which is generally accepted and has proven to correctly describe reflection-induced and injection phenomena for different applications, including feedback interferometry [9, 10].

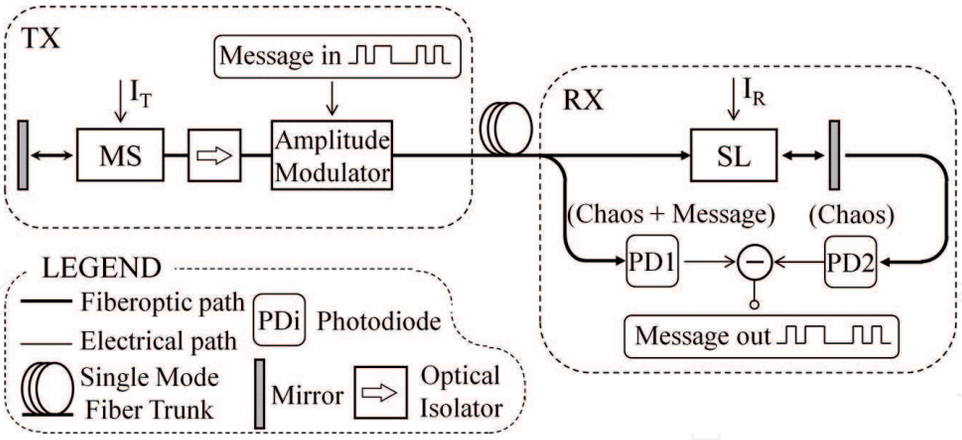

Figure 1. Two-laser scheme of chaos secured transmission (from Annovazzi-Lodi et al. [27]).

Other methods are suitable for chaos generation and synchronization, for example, a two-laser injection system [11, 12]. However, delayed optical feedback is used in virtually all schemes of chaos generation, while direct injection of the master into the slave is preferred for synchronization, since they are by far much easier to implement than other solutions proposed in the literature.

Improved schemes have been also proposed, which use specific methods to better reject eavesdropper attacks [13] or to improve SNR [14], also combining complete and generalized synchronization [15].

Based on this method, data transmission on a metropolitan network [7] has been performed. Several basic functional blocks have been already studied and experimentally demonstrated, such as chaotic signal repeaters [16], subsystems for wavelength multiplexing [17] and for wavelength conversion [18]. Moreover, integrated optics modules for chaotic transmitters and receivers [19, 20] have been designed. A system, specifically designed for transmission on free-space optics links (FSOL), has been presented [21]. Finally, methods to improve masking efficiency [22, 23] and the statistical properties of chaos residual after synchronization, as well as its impact on SNR, have been investigated [24].

Alternatives to the standard approach, still based on delayed optical feedback, have been also studied, and a remarkably different one, using three lasers [25, 26], is shown in **Figure 2**. Here, a common chaotic master laser (driver, DRV) injects two slave lasers (SL1, SL2), one at the transmitter (Tx) and the other at the receiver (Rx). If the two slaves are "twins," and both synchronized to the driver, 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 most important difference between the three-laser and the two-laser secure transmission schemes is that in the three-laser scheme, both SLs are symmetrically injected by the third laser and by their external mirrors, whereas in the two-laser scheme, the master is injected by its own external mirror only, and the slave by its mirror and by the master. Thus, in this second case, the twin devices work in different injection conditions.

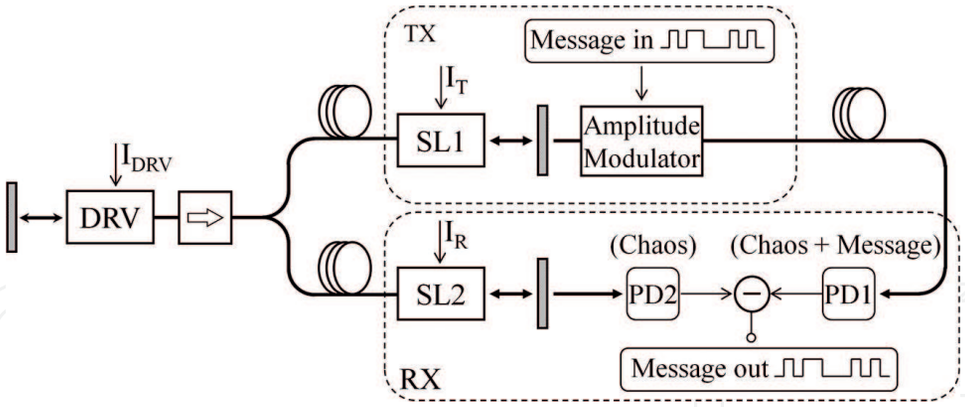

Figure 2. Three-laser scheme of chaos secured transmission (from Annovazzi-Lodi et al. [27]).

3. Comparison of two- and three-laser schemes

Since both the two- and the three-laser schemes have been proposed for secure transmission, it is important to compare their performances [27]. To this end, the bit error rate (BER) and a Q-factor of the optical link have been computed, in back-to-back conditions, as a function of parameter mismatch between Rx and Tx lasers, with the aim of evaluating the quality of the message retrieved by an eavesdropper, after the performance for the authorized sender and recipient has been optimized. This analysis has been carried out by numerical simulations, since selecting many laser pairs, with different combinations of parameters, would result in a very hard experimental effort.

The two-laser scheme (**Figure 1**) and the three-laser scheme (**Figure 2**) have been modeled as detailed in Ref. [27], and the L-K equations are shown below:

$$\frac{dE(t)}{dt} = \frac{1}{2}(1+i\alpha)\left[G(t)-\frac{1}{\tau_p}\right]E(t)+\frac{K}{\tau_{in}}E(t-\tau)\exp(-i\omega\tau)+\frac{K'}{\tau_{in}}E'^{(t-T)}exp(-i\omega T) \quad (1)$$

$$\frac{dN(t)}{dt} = \frac{\eta}{eV}I-\frac{N(t)}{\tau_s}-G(t)|E(t)|^2 \quad (2)$$

$$G(t) = \frac{\xi[N(t)-N_o]}{1-\varepsilon\Gamma|E(t)|^2} \quad (3)$$

In Eqs. (1)–(3), $E(t)$ is the slowly varying, complex electric field of the laser, $N(t)$ the carrier density, $G(t)$ the linear gain, I the pump current, e the electron charge, K is the feedback parameter from MS and SL external mirrors. Other parameters are listed in **Table 1**.

The first term on the right hand side of Eq. (1) together with Eqs. (2) and (3) describes the solitary laser. By adding the second term of Eq. (1), we describe a laser with reflection from an external mirror, that is, all lasers in **Figures 2** and **3**. By also adding the third term in Eq. (1), we describe a laser subject to both reflection and injection from another source, such as the SL

Parameters	Driver	Twin Rx/Tx	Unit
Linewidth enhancement factor	$\alpha = 2.8$	$\alpha = 3$	
Photon lifetime	$\tau_p = 1.9$	$\tau_p = 1.9$	ps
Carrier lifetime	$\tau_s = 1.9$	$\tau_s = 2$	ns
Gain coefficient	$\xi = 7.7\ 10^{-13}$	$\xi = 8\ 10^{-13}$	$m^3\ s^{-1}$
Carrier density at transparency	$N_o = 1.16\ 10^{-24}$	$N_o = 1.10\ 10^{-24}$	m^{-3}
Threshold current	$I_{th} = 12.4$	$I_{th} = 11$	mA
Laser cavity roundtrip time	$\tau_{in} = 8$	$\tau_{in} = 8$	ps
Solitary laser pulsation	$\omega = 1.2177\ 10^{15}$	$\omega = 1.2177\ 10^{15}$	s^{-1}
External cavity roundtrip time	$\tau = 0.3$	$\tau = 0.3$	ns
Active region efficiency	$\eta = 1$	$\eta = 1$	
Active region volume	$V = 8.0\ 10^{-17}$	$V = 8.0\ 10^{-17}$	m^3
Nonlinear gain coefficient	$\varepsilon = 2.5\ 10^{-23}$	$\varepsilon = 2.5\ 10^{-23}$	m^3
Confinement factor	$\Gamma = 0.36$	$\Gamma = 0.36$	
Active medium refractive index	$n = 3$	$n = 3$	
Stimulated emission cross-section	$\zeta = 1.0\ 10^{-20}$	$\zeta = 1.0\ 10^{-20}$	m^2

Table 1. Parameters used for numerical simulations.

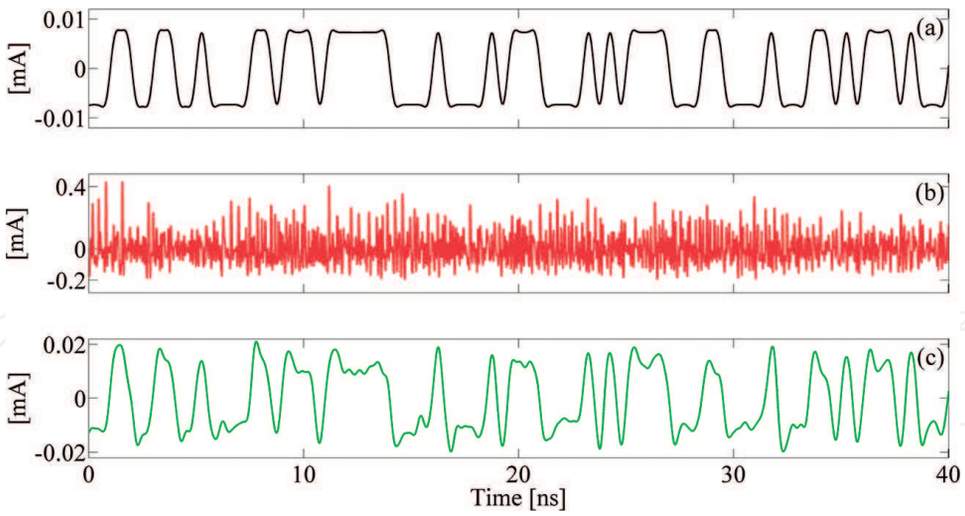

Figure 3. Message in clear (a), message hidden in chaos (b) and recovered message (c) (from Annovazzi-Lodi et al. [28]).

in **Figure 1** and the two SLs in **Figure 2**. The injecting source is described by E′(t), whereas T and K′ are the propagation delay time and the injection parameter between MS and SL, respectively.

In the previous equations, the electric fields are normalized in [$m^{-3/2}$] as usual, and the true value of each electric field (in [V/m]) is given by:

$$E_{true}(t) = \left(\xi\hbar\omega\frac{Z_0}{n\varsigma}\right)^{\frac{1}{2}} \quad (4)$$

where $Z_0 = 1/(\varepsilon_0 c)$ is the vacuum impedance, ε_o is the vacuum permittivity, ħ is the Planck's constant, and c is the speed of light.

In our simulations, we used the typical parameter values [27] shown in **Table 1**. For simplicity, we have taken no propagation delay, T = 0. Langevin noise and photodetector noise (shot noise and Johnson noise of a 50 Ω load resistance) have been taken into account.

We started by assuming perfectly matched pairs for both schemes (i.e., twin MS and SL in the two-laser scheme and twin SL1, SL2 in the three-laser scheme). After selecting a suitable working point, the same for the lasers of both schemes, the message amplitude has been determined in order to get a BER = 10^{-9} for a non-return to zero (NRZ) 2 Gb/s digital signal. This data rate has been selected for the best message protection since the chaos had a broad amplitude maximum at 2 GHz for our devices.

Then, the laser parameters of the L-K model, that is, linewidth enhancement factor α, photon lifetime τ_p, carrier lifetime τ_s, gain coefficient ξ and carrier density at transparency N_0, have been varied by 1% steps, and BER and Q were computed again for all cases. In order to more closely simulate a real experiment for each parameter set, synchronization has been optimized by acting on the pump current of the Rx and on its injection from the MS or DRV laser. This is what the authorized recipient can do to optimize the message quality. This is also what an eavesdropper can do to try to force the cryptosystem.

For example, in **Figure 3**, a simulation of a digital message transmission is shown, assuming a small mismatch (1%) between the parameters of the twin lasers.

In **Figure 3**, the first trace (a) is without both MS and SL external reflectors and represents a measure of the channel transmission quality, which takes into account noise and bandwidth limitations, for reference; the second trace (b) shows message + chaos, whereas trace (c) visualizes the message extracted from chaos after synchronization. Some disturbances, mainly due to residual chaos, are visible on the recovered digital message; however, the message quality can be improved by suitable electronic processing, including filters and an amplitude discriminator, possibly after integration over the bit time.

From numerical simulations, it has been found that the best pair for the three-laser scheme is indeed the twin pair, as usually assumed in the literature, and that the BER rapidly drops with parameter mismatch.

This can be appreciated from **Figure 4**, where we plot the BER and Q values obtained for different parameter mismatch.

In this figure, points are shown, each representing one of all different combinations of parameters. Some points represent laser pairs where all parameters have been changed as shown on the abscissa; other points, pairs where only some parameters have been changed, while other parameters keep their nominal values. The different curves connect BER (and Q) values obtained for the same parameter combinations, with different mismatch amounts. It can be

http://dx.doi.org/10.5772/intechopen.70896

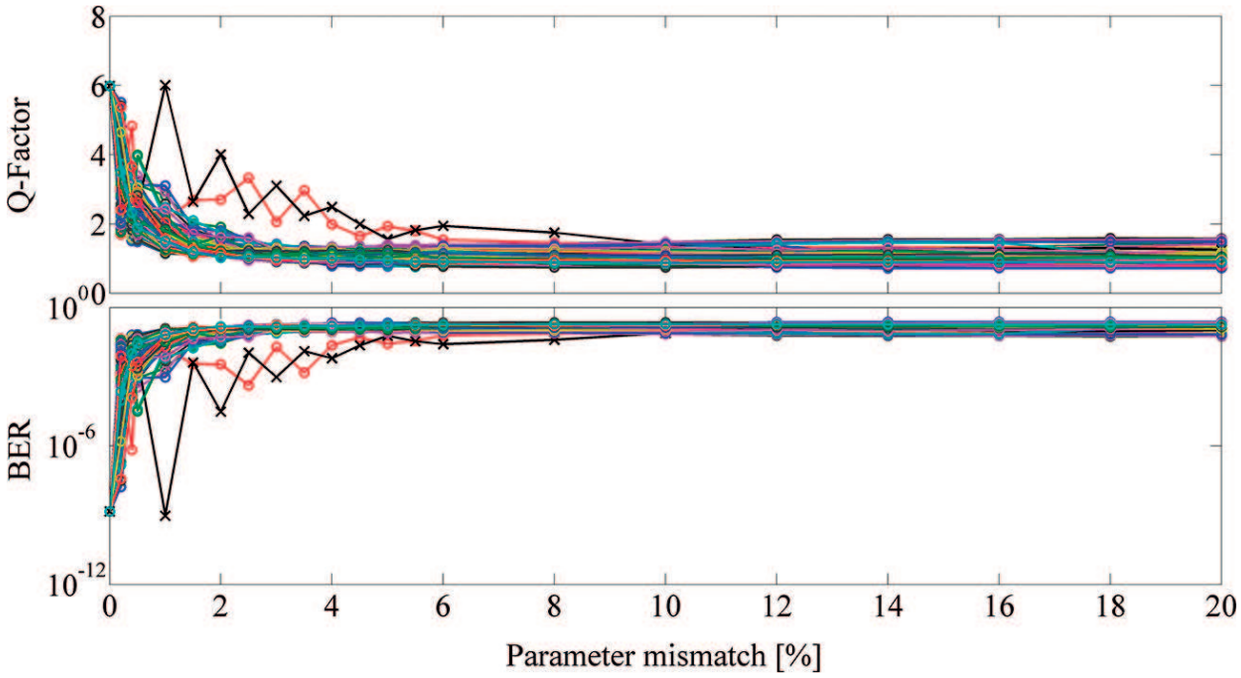

Figure 4. BER and Q as a function of laser parameter mismatch for the three-laser scheme (from Annovazzi-Lodi et al. [28]).

concluded that a mismatch of about 3–4% is enough to strongly reduce the BER, which demonstrates the high level of privacy of the three-laser scheme.

In practice, since it is virtually impossible to find a perfectly matched pair, even for the authorized users, the signal must be somewhat increased to still get low BER even in the presence of a small amount (≈1%) of mismatch. Alternatively, a somewhat higher transmission BER may be accepted by the authorized sender and recipient, who can then improve the BER by a forward error correction (FEC) algorithm. Since such algorithms usually have a threshold in terms of BER, which is difficult to match by the eavesdropper, this results in better transmission privacy.

Different results have been found for the two-laser scheme. In this case, the optimal performance was not obtained using the twin-pair, but, rather, with a pair where all parameters are matched but one, that is, the photon lifetime (curve with the arrow in **Figure 5**), that must be reduced in the SL with respect to the MS. We believe that the reason for this finding is the asymmetry of the two-laser scheme, where the double injection of the slave (by its mirror and by the master), must be compensated by larger cavity losses (i.e., shorter photon lifetime) with respect to the master (being injected by its mirror only).

With our simulated lasers, a reduction of 7% (or 12%) offered the best performances. Thus, we selected this laser pair (with 7% mismatch on photon lifetime) as the new reference and scaled the message amplitude to have BER = 10^{-9} for this optimal pair. The results shown in **Figure 5** for the BER as a function of parameter mismatch were finally obtained.

Figures 4 and **5** allow us to compare the two schemes in terms of privacy and of ease of implementation.

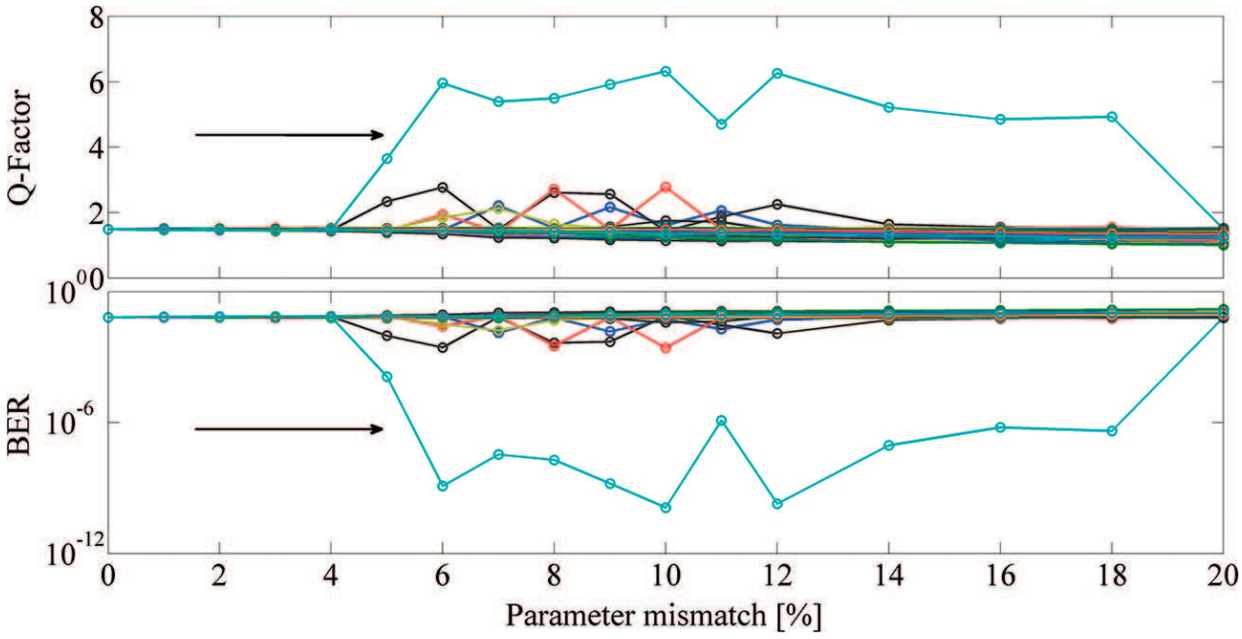

Figure 5. BER and Q as a function of parameter mismatch for the two-laser scheme (from Annovazzi-Lodi et al. [28]).

Since for the two-laser scheme, the authorized sender and recipient have to select a laser with a proper mismatch, they have a more difficult task than with the three-laser scheme, for which the twin pair can be usually found as close-proximity devices on the same wafer. On the other hand, such parameter does not need to be accurately met, which partially simplifies the job.

Once the optimal pair has been selected, the eavesdropper is in a slightly better situation than with the three-laser scheme: s/he has to find a laser similar to another one, without knowledge of its parameters; however, one of these parameters does not need to be accurately matched.

If the authorized sender and recipient prefer to use a twin pair to avoid the problem of selecting the optimal pair, the eavesdropper has the opportunity to extract the message with the same BER as the authorized users, or even better, in principle, if he gets the proper pair. This is not an easy job, however, since an accurate matching of all parameters, but one, is required, without the knowledge of their values. In practice, as it is usually assumed that the eavesdropper cannot match the laser parameters by better than 5%, it is virtually impossible for him/her to extract the message in any case.

4. Chaos-protected network

A common feature of all methods for chaos-protected message transmission is that only point-to-point interconnections between couples of users can be implemented, since a twin pair of lasers is required, one device being used by the transmitter (Tx) and the other by the receiver (Rx). Thus, to exchange data with other subscribers, every user must hold one pair

of twin lasers for each possible correspondent. This is clearly unpractical, especially if the number of users is large.

A more convenient approach [28], similar to public key cryptography, has been proposed recently. By this method, we can build a network of subscribers, where all users can freely exchange data. This configuration is shown in **Figure 6**. The network consists of number of user nodes (US1, US2,…) and also includes a special provider node (PV), whose role is similar to the certifying authority of public-key cryptography.

For each user node US, the network requires a pair of twin lasers. A device of such pair is used by PV, whereas the other by US. The lasers are driven to chaos by a suitable method, such as delayed optical feedback, as in **Figures 1** and **2**.

In **Figure 6**, US1 and US2 are two subscribers at specific network nodes. Each user and the provider share a laser of a twin pair, L1 for US1 and L2 for US2.

If a user (e.g., US1) would like to send a message to another user (US2), s/he starts by sending a message in clear to PV to ask him to create a chaos-protected link.

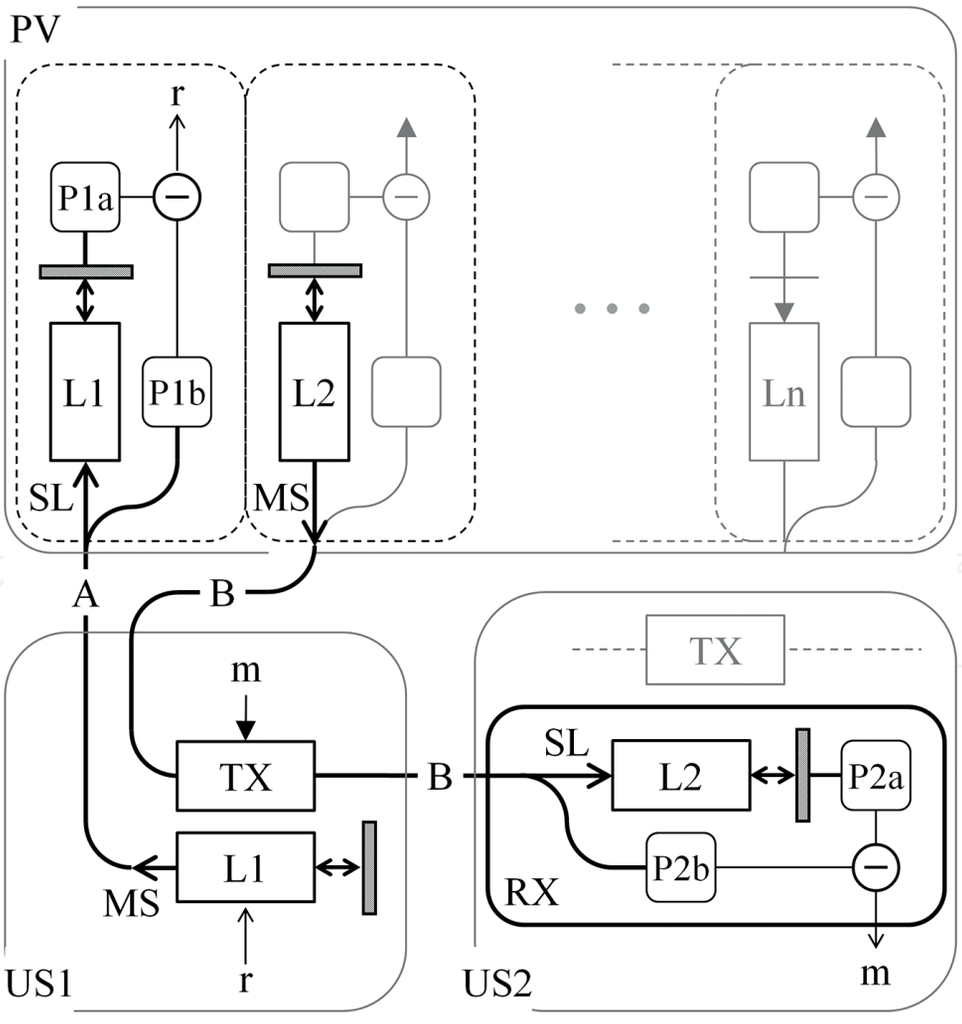

Figure 6. Chaos-protected network. Tx and Rx are the transmitter and receiver blocks and Pij are photodetectors. PV holds one laser for each user, but only L1 and L2 are shown (from Annovazzi-Lodi et al. [28]).

A secure connection from US1 to PV (A in **Figure 6**) is thus established by employing the twin pair held by PV and US1 (L1 in **Figure 6**). This is done by using the standard two-laser scheme, as exemplified in **Figure 6**, or by the three-laser or another suitable scheme.

Then, using the secure link A, US1 sends a message r to PV, asking to create a chaos-secured connection between himself and US2.

After receiving the request of US1, PV sends the chaotic waveform produced by laser L2 to user US1. US1 will use this chaotic carrier to transmit a message m to US2. S/he may use, for example, CM modulation, as in **Figure 6** path B, or another chaos-based transmission method. Exchanged data are protected, since only US2 can extract this message from chaos, because s/he is the only one to hold the required twin laser L2. Other subscribers, or an eavesdropper, cannot retrieve the message.

The same procedure applies, for example, when US2 wants to send a message to US1. US2 first contacts PV in clear; then, using her/his laser L2, s/he asks the provider to route the suitable chaotic waveform (laser L1) to her/him. PV decodes the message by his laser L2 and sends the required chaotic waveform to US2. Using this chaotic waveform, US2 can now send the message, which US1 can decode using her/his laser L1. In the same way, chaos-secured connections can be established between all pairs of users.

Lasers at the provider node are employed either to create a secure connection with a user or to produce a chaotic waveform to be routed to a user to enable her/him to create a secure connection with another user. Lasers at US nodes are used to create a secure connection with the provider or to decode a message of another user. In the proposed network architecture, the traffic between users does not pass by PV node. This is important to improve security and avoid congestion.

The transmission link between two users is usually implemented by simply modulating the chaotic waveform received by the provider, and in such case, only an amplitude modulator is required in block Tx of **Figure 6**. However, if the distance between users, and/or users and PV, is large, amplification of the chaotic waveform is required to adequately hide the message. In such case, an optical amplifier will also be included in block Tx.

Transmission of data between two users following the scheme of **Figure 6** is similar to a standard point-to-point connection. Thus, all the results obtained by the L-K model and by experimental investigations apply here, including our previous comparison of the two basic schemes.

5. Conclusions

In conclusion, after a brief introduction on chaotic cryptography, we have presented recent achievements, by comparing the two most widely used schemes for chaos-secured data transmission, showing that the three-laser scheme has some specific advantage over the two-laser scheme in terms of privacy.

Moreover, we have shown that private transmission based on optical chaos is suitable for multiuser networking, using a proper architecture. This approach is based on the usual, widely investigated and well-developed chaotic transmission schemes, but makes use of a provider to allow for data exchange between several users and requires only one twin laser pair for each subscriber.

Acknowledgements

The authors like to thank Sabina Merlo for fruitful discussions and Andrea Fanzio for technical assistance.

Author details

Valerio Annovazzi-Lodi*, Giuseppe Aromataris and Mauro Benedetti

*Address all correspondence to: valerio.annovazzi@unipv.it

Department of Electrical, Computer and Biomedical Engineering, University of Pavia, Pavia, Italy

References

[1] Schuster HG. Deterministic Chaos. Weinheim: VCH; 1989. 312 p. ISBN 10:35272668626

[2] Ohtsubo K. Semiconductor Lasers: Stability, Instability and Chaos. New York: Springer; 2009. 535 p. DOI: 10.1007/987-3-642-30147-6

[3] Arecchi FT, Puccioni GL, Tredicce JR. Deterministic chaos in laser with injected signal. Optics Communications. 1984;**51**(4):308-314. DOI: 10.1016/0030-4018(84)90016-6

[4] Donati S, Mirasso C. Feature section on optical chaos and applications to cryptography. IEEE Journal of Quantum Electronics. 2002;**38**(9):1137-1196. DOI: 10.1109/JQE.2002801951

[5] Larger L, Goedgebuer JP. Special number on "Criptography using optical chaos". Comptes Rendus de l'Academie des Sciences-Dossier de Physique. 2004;**6**(5):609-681 ISSN: 16310705

[6] Annovazzi-Lodi V, Benedetti M, Merlo S, Norgia M. Fiberoptics setup for chaotic cryptographic communications. Comptes Rendus de l'Academie des Sciences-Dossier de Physique. 2004;**6**(5):623-631. DOI: 10.1016/j.crhy.2004.03.005

[7] Argyris A et al. Chaos-based communications at high bit rates using commercial fiber-optic links. Nature. 2005;**438**:343-346. DOI: 10.1038/nature04275

[8] Lang R, Kobayashi K. External optical feedback effects on semiconductor injection laser properties. IEEE Journal of Quantum Electronics. 1980;**16**(3):347-355. DOI: 10.1109/JQE.1980.1070479

[9] Donati S, Giuliani G, Merlo S. Laser diode interferometer for measurements of displacements without ambiguity. IEEE Journal of Quantum Electronics. 1995;**31**(1):113-119. DOI: 10.1109/3.341714

[10] Annovazzi-Lodi V et al. Optical detection of the Coriolis force on a silicon micromachined gyroscope. Journal of Microelectromechanical Systems. 2003;**12**(5):540-549. DOI: 10.1109/JMEMS.2003.817893

[11] Annovazzi-Lodi V, Donati S. Injection modulation in coupled laser oscillators. IEEE Journal of Quantum Electronics. 1980;**16**(8):859-864. DOI: 10.1109/JQE.1980.1070582

[12] Annovazzi-Lodi V, Donati S, Scirè A. Synchronization of chaotic injected-laser systems and its application to optical cryptography. IEEE Journal of Quantum Electronics. 1966;**32**(6):953-959. DOI: 10.1109/3.502371

[13] Pisarchik AN, Jimenez-Rodriguez M, Jaimes-Reategui R. How to resist synchronization attacks. Discontinuity, Nonlinearity, Complexity. 2015;**4**(1):1-9. DOI: 10.5890/DNC.2015.03.001

[14] Pisarchik AN, Jaimes-Reátegui R, Sevilla-Escoboza JR, Ruiz-Oliveras FR, García-López JH. Two-channel optoelectronic chaotic communication system. Journal of Franklin Institute. 2012;**349**(10):3194-3202. DOI: 10.1016/j.jfranklin.2012.10.005

[15] Pisarchik AN, Ruiz-Oliveras FR. Optical chaotic communication using generalized and complete synchronization. IEEE Journal of Quantum Electronics. 2010;**46**(3):279-284. DOI: 10.1109/JQE.2009.2032429

[16] Lee W, Shore KA. Demonstration of a chaotic optical message relay using DFB laser diode. IEEE Photonics Technology Letters. 2006;**18**(1):169-171. DOI: 10.1109/LPT.2005.860039

[17] Matsuura T, Uchida A, Yoshimori S. Chaotic wavelength division multiplexing for optical communication. Optics Letters. 2004;**29**:2731-2733. DOI: 10.1364/OL.29.002731

[18] Annovazzi-Lodi V, Aromataris G, Benedetti M, Cristiani I, Merlo S, Minzioni P. All-optical wavelength conversion of a chaos masked signal. IEEE Photonics Technology Letters. 2007;**19**(22):1783-1785. DOI: 10.1109/LPT.2007.906847

[19] Syvridis D, Argiris A, Bogris A, Hamacher M, Giles I. Integrated devices for optical chaos generation and communications applications. IEEE Journal of Quantum Electronics. 2009;**45**(11):1421-1428. DOI: 10.1109/JQE.2009.2027336

[20] Tronciu VZ, Mirasso C, Colet P, Hamacher M, Benedetti M, Vercesi V, Annovazzi-Lodi V. Chaos generation and synchronization using an integrated source with an air gap. IEEE Journal of Quantum Electronics. 2010;**46**(12):1840-1846. DOI: 10.1109/JQE.2010.2049642

[21] Annovazzi-Lodi V, Aromataris G, Benedetti M, Merlo S. Secure chaotic transmission on a free-space optics data link. IEEE Journal of Quantum Electronics. 2008;**44**(11):1089-1095. DOI: 10.1109/JQE.2008.2001929

[22] Ursini L, Santagiustina M, Annovazzi-Lodi V. Enhancing chaotic communication performances by Manchester coding. IEEE Photonics Technology Letters. 2008;**20**(6):401-403. DOI: 10.1109/LPT.2008.916918

[23] Aromataris G, Annovazzi-Lodi V. Enhancing privacy of chaotic communications by double masking. IEEE Journal of Quantum Electronics. 2013;**49**(11):955-959. DOI: 10.1109/JQE.2013.2283584

[24] Aromataris G, Annovazzi-Lodi V. Error analysis of a digital message impaired by optical chaos. IEEE Photonics Technology Letters. 2012;**24**(11):903-905. DOI: 10.1109/LPT.2012.2190395

[25] Ohtsubo J. Chaos synchronization and chaotic signal masking in semiconductor lasers with optical feedback. IEEE Journal of Quantum Electronics. 2002;**38**(9):1141-1154. DOI: 10.1109/JQE.2002.801883

[26] Annovazzi-Lodi V, Aromataris G, Benedetti M, Merlo S. Private message transmission by common driving of two chaotic lasers. IEEE Journal of Quantum Electronics. 2010;**46**(2):258-264. DOI: 10.1109/JQE.2009.2030895

[27] Annovazzi-Lodi V, Aromataris G. Privacy in two-laser and three-laser chaos communications. IEEE Journal of Quantum Electronics, DOI. Jul 2015;**51**(7):7109819. DOI: 10.1109/JQE.2015.2434274

[28] Annovazzi-Lodi V, Aromataris G, Benedetti M. Multi-user private transmission with chaotic lasers. IEEE Journal of Quantum Electronics. 2012;**48**(8):1095-1101. DOI: 10.1109/JQE.2012.2202373

IntechOpen