Chaos-on-a-chip secures data transmission in optical fiber links

Apostolos Argyris,[1]* Evangellos Grivas,[1] Michael Hamacher,[2] Adonis Bogris,[1] and Dimitris Syvridis[1]

[1] *Department of Informatics and Telecommunications, National and Kapodistrian University of Athens, Panepistimiopolis, Ilisia, 15784, Greece*
[2] *Fraunhofer Institute for Telecommunications, Heinrich-Hertz-Institute, 10587, Berlin, Germany*
**argiris@di.uoa.gr*

Abstract: Security in information exchange plays a central role in the deployment of modern communication systems. Besides algorithms, chaos is exploited as a real-time high-speed data encryption technique which enhances the security at the hardware level of optical networks. In this work, compact, fully controllable and stably operating monolithic photonic integrated circuits (PICs) that generate broadband chaotic optical signals are incorporated in chaos-encoded optical transmission systems. Data sequences with rates up to 2.5 Gb/s with small amplitudes are completely encrypted within these chaotic carriers. Only authorized counterparts, supplied with identical chaos generating PICs that are able to synchronize and reproduce the same carriers, can benefit from data exchange with bit-rates up to 2.5Gb/s with error rates below 10^{-12}. Eavesdroppers with access to the communication link experience a 0.5 probability to detect correctly each bit by direct signal detection, while eavesdroppers supplied with even slightly unmatched hardware receivers are restricted to data extraction error rates well above 10^{-3}.

OCIS codes: (060.4785) Optical security and encryption; (060.4510) Optical communications.

References and links

1. J. Katz, and Y. Lindell, *Introduction To Modern Cryptography: Principles and Protocols* (Chapman & Hall / CRC Press, 2007)
2. B. Schneier, *Applied Cryptography: Protocols, Algorithms, and Source Code in C* (Wiley, 1996)
3. Federal Information Processing Standards Publication 197, “Announcing the advanced encryption standard (AES),” (2001) *http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf*
4. C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, “Experimental quantum cryptography,” J. Cryptology **5**(1), 3–28 (1992).
5. T. Schmitt-Manderbach, H. Weier, M. Fürst, R. Ursin, F. Tiefenbacher, T. Scheidl, J. Perdigues, Z. Sodnik, C. Kurtsiefer, J. G. Rarity, A. Zeilinger, and H. Weinfurter, “Experimental demonstration of free-space decoy-state quantum key distribution over 144 km,” Phys. Rev. Lett. **98**(1), 010504 (2007).
6. G. D. VanWiggeren, and R. Roy, “Communication with chaotic lasers,” Science **279**(5354), 1198–1200 (1998).
7. P. Colet, and R. Roy, “Digital communication with synchronized chaotic lasers,” Opt. Lett. **19**(24), 2056–2058 (1994).
8. S. Tang, and J. M. Liu, “Message encoding-decoding at 2.5 Gbits/s through synchronization of chaotic pulsing semiconductor lasers,” Opt. Lett. **26**(23), 1843–1845 (2001).
9. K. Kusumoto, and J. Ohtsubo, “1.5-GHz message transmission based on synchronization of chaos in semiconductor lasers,” Opt. Lett. **27**(12), 989–991 (2002).
10. 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 **437**(7066), 343–346 (2005).
11. L. Larger, and J. P. Goedgebuer, “Cryptography using optical chaos,” C. R. Phys. **5**, 609–681 (2004).
12. K. M. Cuomo, A. V. Oppenheim, and S. H. Strogatz, “Synchronization of Lorenz based chaotic circuits with applications to communications,” IEEE Trans. Circuits Syst. II **40**(10), 626–633 (1993).
13. “Introduction to the feature section on optical chaos and applications to cryptography,” IEEE J. Quantum Electron. **38**(9), 1138–1140 (2002).
14. P. Ashwin, “Nonlinear dynamics: Synchronization from chaos,” Nature **422**(6930), 384–385 (2003).

#121683 - $15.00 USD Received 17 Dec 2009; revised 29 Jan 2010; accepted 1 Feb 2010; published 25 Feb 2010

15. C. R. Mirasso, P. Colet, and P. Garcia-Fernandez, "Synchronization of chaotic semiconductor lasers: application to encoded communications," IEEE Photon. Technol. Lett. **8**(2), 299–301 (1996).
16. T. Franck, S. D. Brorson, A. Moller-Larsen, J. M. Nielsen, and J. Mork, "Synchronization phase diagrams of monolithic colliding pulse mode-locked lasers," IEEE Photon. Technol. Lett. **8**(1), 40–42 (1996).
17. S. Bauer, O. Brox, J. Kreissl, B. Sartorius, M. Radziunas, J. Sieber, H. J. Wünsche, and F. Henneberger, "Nonlinear dynamics of semiconductor lasers with active optical feedback," Phys. Rev. E Stat. Nonlin. Soft Matter Phys. **69**(1), 016206 (2004).
18. O. Ushakov, S. Bauer, O. Brox, H.-J. Wünsche, and F. Henneberger, "Self-organization in semiconductor lasers with ultrashort optical feedback," Phys. Rev. Lett. **92**(4), 043902 (2004).
19. M. Yousefi, Y. Barbarin, S. Beri, E. A. Bente, M. K. Smit, R. Nötzel, and D. Lenstra, "New role for nonlinear dynamics and chaos in integrated semiconductor laser technology," Phys. Rev. Lett. **98**(4), 044101 (2007).
20. A. Argyris, M. Hamacher, K. E. Chlouverakis, A. Bogris, and D. Syvridis, "Photonic integrated device for chaos applications in communications," Phys. Rev. Lett. **100**(19), 194101 (2008).
21. L. Shu, and D. J. Jr, Costello, *Error Control Coding: Fundamentals and Applications* (Prentice-Hall, New Jersey, 1983)
22. S. G. Wilson, *Digital Modulation and Coding* (Prentice-Hall, New Jersey, 1996)
23. R. Lang, and K. Kobayashi, "External optical feedback effects on semiconductor injection laser properties," IEEE J. Quantum Electron. **16**(3), 347–355 (1980).
24. J. Mork, B. Tromborg, and J. Mark, "Chaos in semiconductor lasers with optical feedback: theory and experiment," IEEE J. Quantum Electron. **28**(1), 93–108 (1992).
25. H. Olesen, J. H. Osmundsen, and B. Tromborg, "Nonlinear dynamics and spectral behaviour for an external cavity laser," IEEE J. Quantum Electron. **22**(6), 762–773 (1986).
26. J. Sacher, W. Elsasser, and E. O. Gobel, "Nonlinear dynamics of semiconductor laser emission under variable feedback conditions," IEEE J. Quantum Electron. **27**(3), 373–379 (1991).
27. H. Kakiuchida, and J. Ohtsubo, "Characteristics of a semiconductor laser with external feedback," IEEE J. Quantum Electron. **30**(9), 2087–2097 (1994).
28. K. Petermann, "External optical feedback phenomena in semiconductor lasers," IEEE J. Sel. Top. Quantum Electron. **1**(2), 480–489 (1995).
29. J. Ohtsubo, *Semiconductor Lasers: Stability, Instability and Chaos* (Springer, 2007)
30. R. Vicente, J. Dauden, P. Colet, and R. Toral, ""Analysis and characterization of the hyperchaos generated by a semiconductor laser subject to a delayed feedback loop," IEEE. J," Quantum Electron. **41**(4), 541–548 (2005).
31. T. Heil, I. Fischer, W. Elsäßer, B. Krauskopf, K. Green, and A. Gavrielides, "Delay dynamics of semiconductor lasers with short external cavities: bifurcation scenarios and mechanisms," Phys. Rev. E Stat. Nonlin. Soft Matter Phys. **67**(6), 066214 (2003).
32. M. W. Lee, J. Paul, S. Sivaprakasam, and K. A. Shore, "Comparison of closed-loop and open-loop feedback schemes of message decoding using chaotic laser diodes," Opt. Lett. **28**(22), 2168–2170 (2003).
33. L. M. Pecora, and T. L. Carroll, "Synchronization in chaotic systems," Phys. Rev. Lett. **64**(8), 821–824 (1990).
34. L. M. Pecora, and T. L. Carroll, "Driving systems with chaotic signals," Phys. Rev. A **44**(4), 2374–2383 (1991).
35. K. M. Cuomo, and A. V. Oppenheim, "Circuit implementation of synchronized chaos with applications to communications," Phys. Rev. Lett. **71**(1), 65–68 (1993).
36. A. Uchida, M. Shinozuka, T. Ogawa, and F. Kannari, "Experiments on chaos synchronization in two separate microchip lasers," Opt. Lett. **24**(13), 890–892 (1999).
37. H. Fujino, and J. Ohtsubo, "Experimental synchronization of chaotic oscillations in external-cavity semiconductor lasers," Opt. Lett. **25**(9), 625–627 (2000).
38. R. Vicente, T. Pérez, and C. R. Mirasso, "Open-versus closed-loop performance of synchronized chaotic external-cavity semiconductor lasers," IEEE J. Quantum Electron. **38**(9), 1197–1204 (2002).
39. D. Rontani, A. Locquet, M. Sciamanna, and D. S. Citrin, "Loss of time-delay signature in the chaotic output of a semiconductor laser with optical feedback," Opt. Lett. **32**(20), 2960–2962 (2007).
40. J.-G. Wu, G.-Q. Xia, and Z.-M. Wu, "Suppression of time delay signatures of chaotic output in a semiconductor laser with double optical feedback," Opt. Express **17**(22), 20124–20133 (2009).
41. M. C. Soriano, P. Colet, and C. R. Mirasso, "Security Implications of Open- and Closed-Loop Receivers in All-Optical Chaos-Based Communications," IEEE Photon. Technol. Lett. **21**(7), 426–428 (2009).
42. V. S. Udaltsov, J.-P. Goedgebuer, L. Larger, J.-B. Cuenot, P. Levy, and W. T. Rhodes, "Cracking chaos-based encryption systems ruled by nonlinear time delay differential equations," Phys. Lett. A **308**(1), 54–60 (2003).

1. Introduction

Protocol cryptography at the third (internet protocol security - IPsec) and fourth (transport layer security – TLS, or secure sockets layer – SSL) layers of the OSI networking model has been almost a tenet for securing such communication channels [1,2]. Second layer encryption using cryptographic algorithms (e.g. 256-bit advanced encryption standard – AES) is increasingly adopted in the last years for securing military and critical networking infrastructures, offering offload complexity and reducing maintenance charges [1–3]. On the contrary, hardware encryption is practically not yet applied in the conventional optical communication systems; nevertheless it is explicitly investigated in recent years in two different directions, due to its potential to provide an additional security layer. Quantum

#121683 - $15.00 USD Received 17 Dec 2009; revised 29 Jan 2010; accepted 1 Feb 2010; published 25 Feb 2010

cryptography ensures protected links using fundamental laws of physics for secure key distribution [4,5]; however there are some limitations regarding the communicating speed and distance, the ad hoc equipment, etc. Chaos data encryption provides an additional degree of security in software-secured systems. It is based on hardware identical devices and is applied to the physical layer, allowing real-time data encryption [6–11]. While quantum cryptography secures the transmission link and distributes the encryption key, chaos encryption secures each bit of data separately; thus, every eavesdropping attempt does not write-off the communication channel. In communication systems that encrypt high-speed data within broadband chaotic carriers, authorized users share identical chaotic oscillators, capable – after synchronization – of emitting exactly the same chaotic optical signal [12–15]. The complexity of the emitter in terms of design and fabrication parameters, as well as the identification of operating conditions that lead to chaos generation of high dimensionality provides a carrier for real-time encrypted-data transmission.

Built-on-chip chaotic emitters through photonic integration appear very attractive, since they could be easily included in the existing infrastructure of optical networks. Although a few works in the near past presented photonic devices that exhibited interesting nonlinear and chaotic behavior, their low-complexity and narrow-bandwidth emitted signals made them inappropriate for high bit rate data encryption applications [16–19]. On the contrary, a controllable photonic integrated emitter has been presented in [20], where preliminary results proved the feasibility of this device to exhibit complex chaotic dynamics under strictly determined operating conditions.

In this work we report the first demonstration of PIC-based, fully controllable broadband chaotic oscillators, capable of exhibiting an outstanding performance in closed-loop synchronization architectures with extreme stability. We also report the first experimental demonstration of a long-distance optical communication system that exploits the enhanced efficiency of closed-loop synchronization of the above PICs, for secure 2.5 Gb/s data exchange with bit-error-rates below 10^{-12}. Such low BER values are achieved only for authorized users, even for very small encrypted message amplitudes, through forward error correction (FEC) techniques [21,22]. The FEC method used in our system poses a digital bit-error-rate threshold ($\Re = 1.8 \cdot 10^{-3}$) in its operation, discriminating decisively the data recovery efficiency between authorized and unauthorized users. The latter, either by direct detection of transmission line or by employing unmatched – compared to the PIC emitter – hardware receivers, will be able to recover data with BER values as low as this digital threshold $\Re$. The above achievements show the potential of chaos encoding approach to be seamlessly integrated in the existing point-to-point optical communication links.

2. Chaos generation and synchronization

The proposed PIC, as shown in Fig. 1, has been fabricated using selective area epitaxial growth and incorporates the fundamental principles of the time-delayed all-optical feedback theory [23–29], using different sections that provide the capability to control the chaotic properties of the optical emission accurately and reproducibly. Criterion for the selection of the short external cavity length is the ability of the device to produce chaotic attractors with high complexity. The selected length of 1cm corresponds to a feedback round-trip time of approximately 280 ps, a delay long enough – as forecasted by theory and numerical predictions – to provide a fully chaotic behavior [30,31]. Depending on the biasing current of the DFB laser and the feedback strength, the bandwidth of the chaotic carrier may be increased from several GHz up to 20 GHz. The integration of an amplifying / absorbing (SOA / VOA) section offers control on the feedback strength; no biasing of this section leads to a specific optical power feedback ratio equal to 1.6%, which is predetermined by the inherent losses of the external cavity. Even though the last value proves to be high enough to generate chaotic dynamics, the feedback ratio can be increased up to 5% by positively biasing the SOA section for increased complexity. The phase section (PM) accurately tunes the round-trip time of the cavity with sub-wavelength resolution; this operation is extremely crucial for synchronization with other matched devices that might exhibit a small mismatch in the cavity

#121683 - $15.00 USD Received 17 Dec 2009; revised 29 Jan 2010; accepted 1 Feb 2010; published 25 Feb 2010

length. Precise thermo-electric cooling of the devices, by using the appropriate packaging for the PICs, provides controllability and operating long-term stability, not only in terms of wavelength and optical power, but also in terms of the spectral distribution of the chaotic carrier and the phase matching conditions. All the above are vital parameters for the accomplishment of high-performance closed-loop synchronization [13,32].

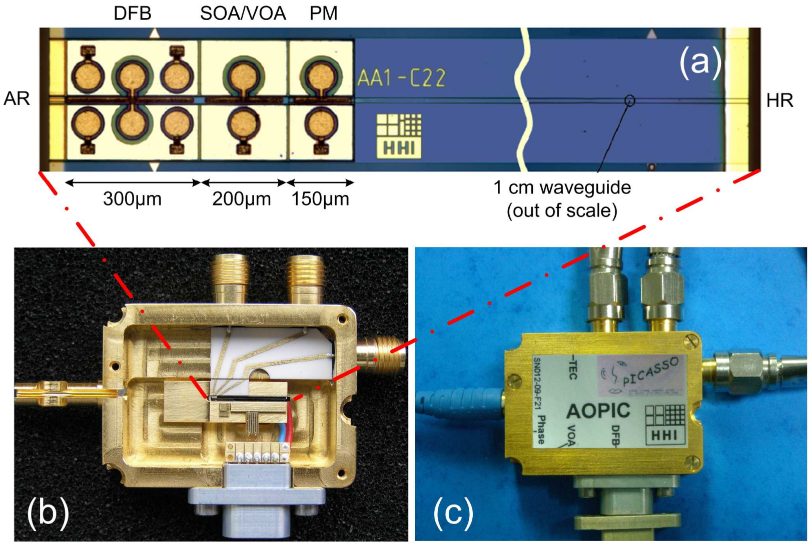

Fig. 1. Photonic monolithic integrated chaos generator: (a) The device consists of a DFB laser that forms an external optical cavity with the rear facet of the PIC that is highly reflective coated (HR); the cavity also includes various active/passive sections, such as a variable gain/absorption section (SOA/VOA), a phase section (PM) and a 1cm-long waveguide. The output optical signal is emitted from the front anti-reflective (AR) facet of the DFB laser. (b) Internal structure of the packaging module: Micro-strip lines connect the different active sections of the PIC with SMA connectors, while thermo-electric cooling of the device provides extremely stable temperature control. Fiber-chip coupling is performed by a tapered-end fiber with antireflective coating. (c) Packaged module.

Synchronization of chaotic circuits has been ardently demonstrated in the past [12,33–37] revealing the necessity of identity between the coupled oscillators in order to accomplish efficiently the reproduction of chaotic sequences. Especially when such oscillators become more complex and sophisticated in terms of their design, fabrication and operating conditions, the route to chaos synchronization is not furthermore straightforward. The PIC modules employed in this work support closed-loop receiver configurations, which presume at the receiver a PIC replica of the emitter. In a case of comprehensive device identity, enhanced synchronization performance can be obtained, compared with open-loop receiver architectures that incorporate only an identical laser section and exclude the existence of any external cavity [38]. This discrepancy accredits increased security in closed-loop communication systems, since an eavesdropping receiver becomes more demanding in its specifications. The standardized fabrication process of the designed PICs guarantees a tolerable matching of the internal parameters, the operating characteristics and the external cavity length for all devices; however, even from the same fabrication wafer, only a few matched-pairs out of dozens of devices prove to be identical in order to provide efficient closed-loop synchronization. A simple way of evaluating the synchronization quality of these carriers is by measuring their cancellation efficiency, after converting the chaotic optical signals into electrical signals and measuring the electrical cancellation coefficient $c^{E}_{\Delta f}$, which is defined as:

$$c^{E}_{\Delta f}(dB) = \left\langle \left| P^{E}_{t}(f) \right| \right\rangle \Big|_{\Delta f} (dBm) - \left\langle \left| P^{E}_{t}(f) - P^{E}_{r}(f) \right| \right\rangle \Big|_{\Delta f} (dBm) \qquad (1)$$

#121683 - $15.00 USD Received 17 Dec 2009; revised 29 Jan 2010; accepted 1 Feb 2010; published 25 Feb 2010

$P_t^E(f)$ and $P_r^E(f)$ are the electrical power values of the transmitter and the receiver output in a specific frequency f. In Eq. (1) the averaging is performed in the frequency domain and refers to the frequency bandwidth Δf of the carrier. As identified from the study performed, the similitude of the spectral distribution of the selected matched-pair carriers is a practical guideline for achieving efficient synchronization. A pair of chaos-generating PICs with minor mismatches – below 5% in their internal and operating parameter values, as well as in their spectral emission profiles – has been selected to serve as transmitter / receiver subsystems, providing efficient data encryption at the emitter side and data extraction at the receiver side. In the two cases shown in Figs. 2(a) and 2(b), an uncoupled pair of matched PICs taken from the same wafer provides almost the same spectral profile distribution (emitter: black line, receiver: red line), by applying the appropriate operating conditions. After coupling the PICs unidirectionally, by injecting a small amount of optical power from the emitter to the receiver – up to 3 times the optical feedback of the PICs – chaos cancellation between the two signals (blue line) overcomes even 20dB in some narrow spectral regions. Electrical cancellation coefficient values as high as 16dB have been measured in a 10-GHz bandwidth, which means that when used in a transmitter-receiver configuration the chaotic carrier signal finally will be eliminated at a ~97% ratio. On the contrary, even in matched-pair PICs, any slight discrepancy on the emitted spectral profiles due to improper operating conditions leads to degraded cancellation performance after coupling [Fig. 2(c)]. In such a case, fine tuning of the PICs' control parameters that affect the spectral distribution of the emission can balance the spectral matching and improve synchronization [Fig. 2(d)].

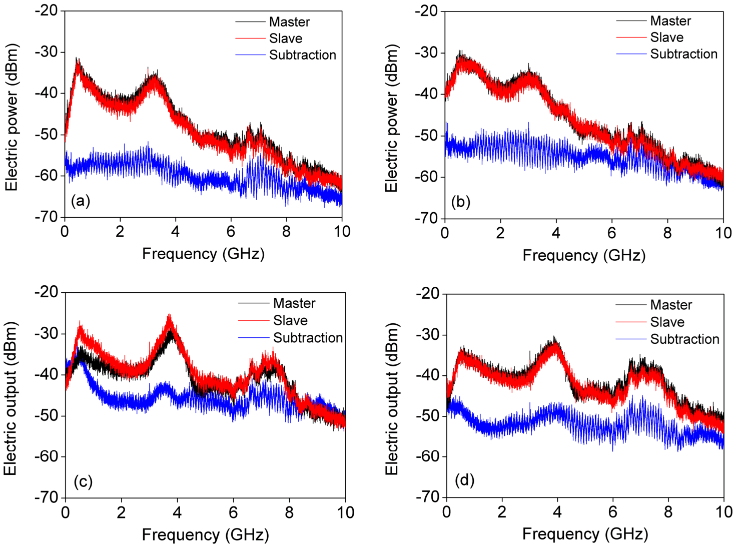

Fig. 2. Synchronization between chaotic carriers emitted by matched-pair PICs: Spectral distribution of the chaotic signals emitted by the emitter's PIC (black), the receiver's PIC (red) and their subtraction at the receiver (blue) for various operating conditions: (a) $I_{L,M}$ = 30mA, $I_{L,S}$ = 26.5mA, $V_{VOA,M,S}$ = 0V, $I_{PH,M}$ = 3mA, $I_{PH,S}$ = 0mA. (b) $I_{L,M}$ = 30mA, $I_{L,S}$ = 26.5mA, $V_{VOA,M,S}$ = 0V, $I_{PH,M}$ = 4.8mA, $I_{PH,S}$ = 0.2mA. (c) $I_{L,M}$ = 25mA, $I_{L,S}$ = 22.7mA, $I_{SOA,M,S}$ = 0.1mA, $I_{PH,M}$ = 3.8mA, $I_{PH,S}$ = 0mA. (d) $I_{L,M}$ = 25mA, $I_{L,S}$ = 22.7mA, $I_{SOA,M}$ = 0.1mA, $I_{SOA,S}$ = 1.1mA, $I_{PH,M}$ = 3.6mA, $I_{PH,S}$ = 0mA. [$I_{L,i}$: DFB laser current, $V_{VOA,i}$: absorber reverse voltage, $I_{SOA,i}$: amplifying section current, $I_{PH,i}$: phase section current, i: M(master), S(slave)]

Table 1, summarizes the performance of the cases presented in Fig. 2, in terms of $c^E_{\Delta f}$, for two different signal bandwidths. The 10-GHz bandwidth is the full detection bandwidth of the system – limited by the bandwidth of the photoreceivers –, while the 2.5GHz bandwidth covers the spectral region of interest in the communication system of Fig. 3 that supports data rates up to 2.5Gb/s. The lack of powerful high-frequency chaotic components (over 5GHz) and the more efficient synchronization in the low-frequency chaotic components (up to

#121683 - $15.00 USD Received 17 Dec 2009; revised 29 Jan 2010; accepted 1 Feb 2010; published 25 Feb 2010

4GHz) result in the increased values of $c^{E}_{2.4GHz}$ compared to the corresponding c^{E}_{10GHz} values of Table 1.

Table 1. Electrical cancellation of the chaotic carriers of Fig. 2, when employing different bandwidth and synchronization conditions

Synchronization conditions	**Chaotic carrier electrical cancellation coefficient $c^{E}_{\Delta f}$ (dB)**	
	Δf: DC-10GHz	**Δf: DC-2.5GHz**
Figure 2a	16.0	17.7
Figure 2b	14.4	16.7
Figure 2c	4.6	5.1
Figure 2d	11.0	12.1

Depending on the operating conditions of the PICs different radio-frequency spectral distributions of the chaotic carriers can be obtained. For data encryption applications, the appropriate ones emerge from the task to conceal all the spectral components of the transmitted messages. Data series that are encoded by baseband modulation in these carriers request powerful chaotic components in their covering spectral region. At the same time, an optimized synchronization of the system should be preserved. Operating conditions that correspond to the cases presented in Figs. 2(a) and 2(b) favor the above prerequisites, with $c^{E}_{2.4GHz}$ values over 16dB (Table 1).

In a communication system approach, the existence of an encrypted message is expected to influence the synchronization performance, by reducing the final cancellation efficiency. However, small message amplitudes encrypted in such systems – up to 12% of the carrier's mean optical power – cause a minor degradation in cancellation efficiency up to only 1-2dB, as it will be shown in the next section. Given that a recovered message with 12dB SNR can be detected with error rates below 10^{-12}, the cancellation performance provided by the studied PICs can be considered sufficient.

#121683 - $15.00 USD Received 17 Dec 2009; revised 29 Jan 2010; accepted 1 Feb 2010; published 25 Feb 2010

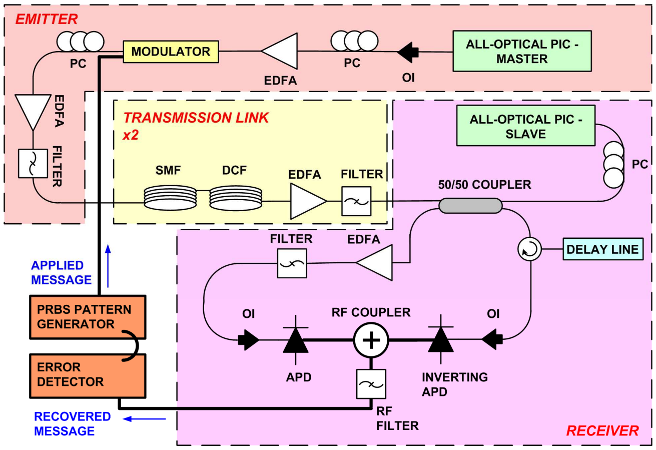

Fig. 3. Topology of the chaos-secured data transmission experiment using PIC chaos generators: Data sequences are applied on the chaotic carrier generated by the emitter's PIC (master) through external modulation. After 100km fiber transmission in dispersion compensated links, 150μW of the transmitted chaotic signal is injected at the receiver's PIC (slave) forcing it to synchronize to the chaotic dynamics of injected input. The subtraction between the transmitted chaotic carrier with the encrypted message and the locally generated chaotic carrier at the receiver leads to chaotic carrier cancellation and electric data recovery. (thin lines: optical fibers, thick lines: electrical cables, OI: optical isolator, PC: polarization controller, EDFA: erbium-doped fiber amplifier, SMF: single mode fiber, DCF: dispersion compensating fiber, 50/50: optical coupler, APD: avalanche photoreceiver).

3. Experimental setup

The structure of a 100-km transmission communication system based on chaotic carriers has been implemented and is illustrated in Fig. 3. Both PICs, selected at the emitter and the receiver, emit optical carriers exactly at 1556.111 ± 0.001nm and their operating conditions correspond to the case of Fig. 2(b). The encoded data are PRBSs with tunable amplitude and 2^{31}-1 length and are applied externally using a 10Gb/s LiNbO3 electro-optic modulator. The optical signal is amplified by an EDFA, followed by a bandpass optical filter – in order to suppress amplified spontaneous emission – and launched into the transmission link. Two identical dispersion-compensated transmission links in series, each one consisting of 50km SMF, 6km DCF and the prerequisite amplification stages, channel the chaos encrypted data to the receiver. The optical power of a broadband signal that is sent for transmission in fiber links of tens or hundreds of km is a crucial parameter. Optical signals with low power are vulnerable to the noise coming from the amplifiers, while high-power optical signals trigger non-linear effects that alter the transmitted chaotic waveforms. Both extreme cases result in a worse synchronization performance at the receiver. The best synchronization performance was attained for an input optical power between 2.5mW and 4.5mW. Thus, an optimal value of 4mW was considered in order to preserve the power of the signal as high as possible and, at the same time, to minimize the effects of the transmission impairments. The receiver synchronizes only to the fluctuations of the chaotic signal after injecting a small fraction – up to 3 times the emitter's PIC optical feedback power - of the transmitted signal into the receiver's PIC. The temporal alignment – through an optical delay line - and power equalization – through amplification – of the two signals driven to the receiver's different optical paths lead to chaotic carrier cancellation and electric data recovery. The subtraction is practically performed by adding the electrically converted signals, after inverting the emitter's one by using an inverting photoreceiver. The appropriate microwave filters have been used at the recovery stage to suppress the undesirable residual spectral components coming from the subtraction and always the bandwidth is matched to the data bit rate: 1.1GHz, for 1.25Gb/s and 2 GHz, for 2.5Gb/s data respectively.

#121683 - $15.00 USD Received 17 Dec 2009; revised 29 Jan 2010; accepted 1 Feb 2010; published 25 Feb 2010

The philosophy of the presented communication system is twofold. On one hand, the emitter sends a completely hidden data stream within a chaotic carrier along the transmission link, and this is achieved – for a specific chaotic carrier – by restricting the message amplitude up to a maximum value. On the other hand, the receiver has the task to cancel the chaotic carrier and recover data with a native bit-error rate as low as needed in order to acquire error rates below 10^{-12} using coding techniques. The BER improvement is achieved by an additional processing unit that employs a fast transceiver which enables FEC methods.

The transceiver used for pattern generation and error detection was part of the FPGA device and was set in order to comply with different commercial standards, such as Gigabit Ethernet and Sonet/SDH. At the receiver, it performs clock and data recovery of the incoming bit stream. For the bit rate of 1.25Gb/s it was configured to be Gigabit Ethernet compatible, while for the bit rate of 2.5Gb/s it was configured to comply with Serial RapidIO. In both cases the 8B/10B encoding/decoding circuitry was deactivated and the PRBS length was not affected.

The FEC method used for improving the inherent recovered data employed the Reed-Solomon (RS) code (255,223), where 32 check symbols were added to every 223 symbols of useful information, leading to an overhead of 14.35%. The size of the Galois field used is 28 (256) with 8-bit long symbols. This configuration allows the correction of up to 16 symbols per codeword (255 symbols), meaning that an error free operation can be achieved while the input BER is as high as 6.3×10^{-2}. This theoretical threshold value applies to the ideal situation where there are exactly 16 erroneous symbols in every codeword. For the specific system studied the threshold value was found to be $\Re = 1.8 \cdot 10^{-3}$ due to burst errors. The effective data rates for the plain link rates of 1.25Gb/s and 2.5Gb/s are 1.09375Gb/s and 2.1875Gb/s respectively. The FEC scheme was implemented along with the BER tester in a Field Programmable Gate Array (FPGA) device (Altera, Stratix II GX EP2SGX90).

4. System performance

Small message amplitudes that externally modulate the chaotic carrier can be completely hidden within the chaotic signal. The message amplitude is of high importance in this encryption technique, providing a twofold benefit: low message amplitudes cannot be distinguishable by tapping the transmission line and are not susceptible to filtering, while at the same time they favor successful recovery only by an authorized user with an identical receiver. Small-amplitude data sequences with SNR as low as 12dB may lead to partial recovery, which can be significantly improved to error rates below 10^{-12} using forward error correction (FEC) techniques [21,22].

The evaluation of this system in terms of data encryption and recovery is performed through bit-error-rate (BER) versus the applied message amplitude, as presented in Fig. 4. This analysis does not follow the typical form of BER curves that characterize conventional optical communication systems which is expressed versus the optical power at the receiver. In the present work the major investigation is to simultaneously achieve data encryption along the transmission line and efficient data recovery – post-processed to BER values lower than 10^{-12} – by an authorized receiver.

#121683 - $15.00 USD Received 17 Dec 2009; revised 29 Jan 2010; accepted 1 Feb 2010; published 25 Feb 2010

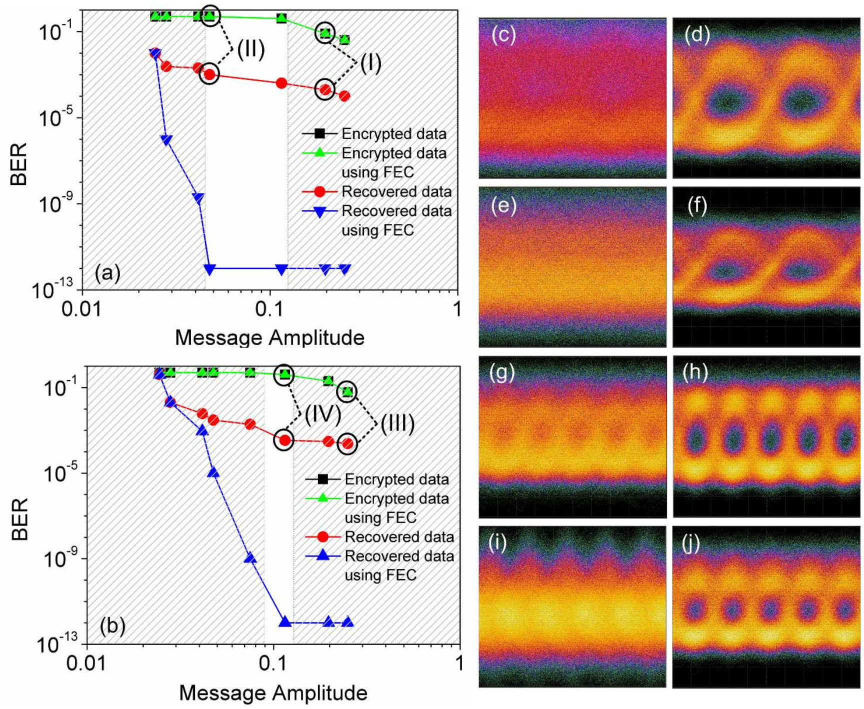

Fig. 4. System performance in terms of data encryption and recovery: Bit-error-rate (BER) measurements vs. data amplitude for (a) 1.25Gb/s and (b) 2.5Gb/s PRBS. The eye-diagrams for the encrypted (left column) and recovered (right column) data that correspond to the cases I-IV of (a) and (b) are shown successively ((c)-(j)). Cases II and IV are selected within an operating window that ensures complete encryption with BER~0.5 [(e) and (i)], while the recovered data have an inherent BER value below 10^{-3} [(f) and (j)] that is enhanced by FEC methods to error free operation. For larger message amplitudes (cases I and III) the probability of error for the encrypted data is below 0.5 [(c) and (g)] providing reduced security, however maintaining an error-free data recovery.

In Fig. 4(a), a 1.25Gb/s data stream is characterized vs. its modulation amplitude, dignifying three different operating regions. The first one involves large message modulation amplitudes (over 12%) of the chaotic carrier's mean optical power. Such amplitude values provide efficient data recovery, with inherent BER values below $\Re = 1.8\cdot10^{-3}$ (case I). The $\Re$ error threshold value determines if, by applying a FEC stage using the appropriate transceiver, a BER value of at least 10^{-12} will finally emerge. However, such large amplitudes act at expense of the quality of message encryption which is below 0.5, indicating that an eavesdropper could extract some bits with direct detection. The second operating region – with message amplitudes from 12% down to 4.5% – ensures what is desired: encryption level that corresponds to a tapped BER value equal to 0.5, recovered data at the receiver with an inherent BER below the $\Re$ value and an after-FEC BER performance of 10^{-12} at maximum (case II). Finally, even smaller amplitudes (below 4.5%) that also preserve secure data encryption cannot lead to efficient recovery, since the inherent BER values are above the value $\Re$, providing errors at the decoding process even for the authorized receiver that uses the FEC technique.

An analogous study is performed after doubling the data rate to 2.5Gb/s, as presented in Fig. 4(b). The extended bandwidth of the message induces a different encryption efficiency compared to the previous case; however, as previously, large message amplitudes cannot be sufficiently encrypted (case III). A secure transmission can be obtained – in a much narrower operating window of amplitude values around 10% – with a 0.5 level encryption and an after-FEC satisfactory performance (case IV).

When omitting the transmission link – working thus in a back-to-back configuration – the BER performance is exactly the same for the case of 1.25Gb/s data streams and faintly better (less than an order of magnitude) for the case of 2.5Gb/s. This behavior validates that transmission does not induce its impairments in low data rates. Such results indicate that probably a much longer transmission link could be employed, without affecting the final performance of the specific communication system.

The above performance analysis is in the main axis for claiming an additional layer of security in optical communication systems, discriminating the following three cases which are also summarized in Table 2:

i) The authorized user is supposed to have access to an identical to the emitter receiver hardware. After efficient closed-loop synchronization, performance data recovery will occur. The non-fixed parameter in this case is the message amplitude applied at the emitter. For security reasons the message amplitude at the emitter is set to such low values that allow the authorized receiver to recover a native BER just below $\Re$ threshold. This BER value is the *"digital threshold"* set for the security of the system, is associated to the operating characteristics of the FEC method and when applied in the system pushes down the BER values to 10^{-12}. As it can be concluded from the performance of the examined system in Fig. 4, the message amplitude should be set to 4.5% for 1.25 Gb/s data series, and 10% for 2.5 Gb/s data series.

ii) Unauthorized users can employ any type of receiver in order to attempt synchronization and data extraction. The only way is to use solitary lasers in an open-loop configuration, since closed-loop receivers assume exact knowledge of the emitter's cavity roundtrip time. In almost all the chaotic optical oscillators that have been presented so far in the literature, long external cavities provide evidence about their roundtrip time though the external cavity modes in their spectral profile. In the presented PIC this is not the case; the roundtrip time corresponds to a frequency around 3.3 GHz and is hidden within the relaxation frequency of the laser that lies in the same region. In such a way, the information for a key parameter of the encryption system, such as the time-delay signature of the PIC's external cavity, is lost [39,40]. A critical test in order to cover this category of users was performed. The authorized PIC of the receiver was operated it in an open-loop configuration, by biasing negatively the SOA/VOA section in order to minimize the optical feedback. The best values for the recovered BER were $2{\cdot}10^{-2}$ and $8{\cdot}10^{-2}$, for bit rates of 1.25Gb/s and 2,5Gb/s, respectively. This is attributed to a worse synchronization performance (c^{E}_{10GHz} is estimated to be 3 dB less when compared with the case of closed-loop configuration), as also predicted in [41]. This study resembles the case that an eavesdropper has exactly the same laser with the emitter, but does not have any information about the external cavity. Even in this case, the eavesdropping receiver fails to exceed the FEC threshold limit $\Re$ and thus improve the decoding performance. An even worse performance is expected for all other lasers that will have some discrepancies in respect to the emitter's PIC laser.

iii) Finally, unauthorized users that may gain access to the transmission line by tapping the physical medium should only be capable - after linear or non-linear filtering - of recovering data with BER values of ~0.5. This value practically means total randomness of the extracted bits. Some attempts in the recent past provided evidence that one could crack chaos-based encryption systems that were based in nonlinear time delay differential equations [42]. Such systems are, for example, the electro-optical chaotic systems, where the non-linearity is imposed using a nonlinear element with well-defined and reproducible non-linearity, such as a Mach-Zehnder modulator. The PICs used in this work include the non-linearity in the laser which is subject to optical feedback. The usage of purely nonlinear filtering approaches would not help, as their effectiveness is under consideration in well encrypted

#121683 - $15.00 USD Received 17 Dec 2009; revised 29 Jan 2010; accepted 1 Feb 2010; published 25 Feb 2010

messages (BER~0.5). Even if an eavesdropper found a way to extract the critical parameters of the device, through software techniques, he would face major difficulties in fabricating an identical device that would comply with his theoretical findings.

Table 2. Security allocation of different types of users via their decoding performance

		Decoding performance	
Type of user	**Action performed**	**Native BER**	**BER after FEC**
Authorized	Identical hardware receiver	$< \Re$	$< 10^{-12}$
Unauthorized	Non-identical hardware receiver	$> \Re$	$> \Re$
Unauthorized	Carrier filtering	~0.5	~0.5

Finally, an essential issue for exploiting such systems in real-world conditions is their operational stability and sustainability over long periods of time. Chaotic carriers should preserve their characteristics that ensure the initial encryption, while synchronization between chaotic carriers after including transmission links should be precisely controlled. A stability analysis performed in the presented system showed that the incorporated chaotic PICs proved to be a reliable solution in terms of securing fiber transmission links, after operating continuously for hundreds of hours, guaranteeing thus a stable encryption and recovery performance.

5. Conclusions

Compact monolithic PICs that generate complex chaotic carriers are tested in optical transmission systems in order to provide an extra layer of security in real-time data exchange. An exremely stable, closed-loop synchronization of high quality is demonstrated for the first time in chaotic systems that include 100km of transmission path. Gb/s data sequences with small modulation amplitudes are totally encrypted within these chaotic carriers. Authorized counterparts supplied with identical PICs and a FEC module can benefit data exchange BER of 10^{-12}, for bit-rates up to 2.5Gb/s. On the contrary, eavesdroppers that tap the transmission line or unauthorized users supplied with mismatched hardware receivers experience a poor BER detection performance that cannot be further improved with FEC processing. Therefore, reliable photonic integrated chaos emitters are now available to be directly and efficiently incorporated as optical transceiver modules in installed systems – being completely transparent to the upper network layers – for high-speed encrypted-data transmission.

Acknowledgements

The authors acknowledge financial support by the E.U. through the project FP6-IST-34551-PICASSO.