Available online at www.sciencedirect.com

SCIENCE DIRECT®

C. R. Physique 5 (2004) 633–642

COMPTES RENDUS

PHYSIQUE

Cryptography using optical chaos/Cryptographie par chaos optique

A short external cavity semiconductor laser cryptosystem

Michael Peil, Ingo Fischer, Wolfgang Elsäßer

Institute of Applied Physics, Darmstadt University of Technology, Schloßgartenstraße 7, 64289 Darmstadt, Germany

Presented by Guy Laval

Abstract

Semiconductor lasers with delayed optical feedback are well-suited for controlled generation of high-dimensional broad-band chaotic emission dynamics. Such dynamics qualify for application as carriers in modern chaos cryptosystems. We analyze the dynamics in dependence on relevant system parameters and find excellent carrier properties for systems operating in the short cavity regime (SCR). We are able to synchronize a solitary receiver laser to such a transmitter and find good Chaos-Pass-Filter properties revealing the high potential of the SCR-dynamics for chaos cryptosystems. We highlight this by demonstrating the successful encrypted transmission of a digital message. ***To cite this article: M. Peil et al., C. R. Physique 5 (2004).***

Résumé

Un système cryptographique à laser à semi-conducteurs à courte cavité. Les lasers à semi-conducteurs avec contre-réaction optique représentent un bon moyen de générer d'une manière controllable une émission chaotique de haute dimension et de large bande. Ces performances les qualifient à être utilisées pour des systémes de cryptage chaotique. Nous étudions l'influence des paramètres du système sur la dynamique et démontrons que le régime de courte cavité (short cavity regime, SCR) peut très bien servir à transmettre des données. Nous démontrons la synchronisation d'un laser récepteur à un émetteur et un filtrage « passe chaos » très effectif, indiquant que le régime de cavité courte offre un grand potentiel pour la cryptographie par chaos. Ces résultats sont affirmés par notre démonstration de la transmission cryptée d'un message digital. ***Pour citer cet article : M. Peil et al., C. R. Physique 5 (2004).***

Keywords: Semiconductor laser; Delayed feedback; Chaos; Short cavity regime; Synchronization; Secure communication

Mots-clés : Laser à semi-conducteurs ; Systèmes à retard ; Chaos ; Régime à courte cavité ; Synchronisation ; Communication par cryptographie chaotique

1. Introduction

In the last two decades there has been a rapidly growing interest in chaos synchronization phenomena. Initially, research was motivated mainly by the intention to understand the mechanisms of the counterintuitive possibility to synchronize the dynamics of independently chaotic dynamical systems when introducing a coupling mechanism [1,2]. A variety of fascinating synchronization phenomena [3] has been discovered in various areas of science, e.g. in physics [4,5], chemistry [6], biology [7] and physiology [8,9]. Their occurrence has attracted much interest and boosted research in this very active branch of nonlinear science. Beyond the interest from the fundamental-science point of view, chaos synchronization phenomena offer novel concepts for feasible applications [10,11].

E-mail address: michael.peil@physik.tu-darmstadt.de (M. Peil).

1631-0705/$ – see front matter © 2004 Académie des sciences. Published by Elsevier SAS. All rights reserved.
doi:10.1016/j.crhy.2004.05.002

Chaos communication is one of the versatile auspicious applications utilizing chaos synchronization phenomena. The basic idea of using chaotic signals as message-carriers for data transmission was introduced by Pecora and Carol in 1990 [1]. Chaos communication systems can be considered as a generalization of conventional communication systems in which a message is modulated onto a periodic transmitter carrier-signal, termed carrier in the following, and sent to a receiver. Detailed knowledge about the carrier is essential for successful message recovery. Some advanced spread-spectrum communication techniques apply carriers with broad-band frequency spectra in order to reduce the liability of the transmission-system towards spectral disturbances. In compliance with this, carriers generated by chaotic transmitters are also broad-band which is an intrinsic property of chaotic dynamics. Therefore, they are potential carriers for reliable communication systems. Furthermore, chaotic carriers with maximum frequencies distinctly beyond 10 GHz can be realized allowing for multi-Gbit/s rate data transmission. The peculiarity of chaos communication systems lies in the message extraction process which is based on synchronization phenomena. These phenomena are required for successful message extraction, since only synchronized receivers are capable of discriminating the message and the chaotic carrier [12,13]. This is a major advantage of chaos communication systems, because only a receiver very similar to the transmitter, in parameters and operation conditions, can synchronize to the chaotic carrier. Hence, the knowledge about the receiver structure and its operation parameters provides a key which is required for message extraction. This means that a chaos communication system is a cryptosystem which enables message encryption on the physical layer, thus being a complementary approach to software encryption.

Up to now, a variety of message encoding techniques has been introduced. Some well-known are Chaos-Shift-Keying (CSK), Chaos-Modulation (CM), Chaos-Masking (CMK) and ON/OFF-Shift-Keying (OOSK). A brief overview is given in [15,16] and in the references cited therein. One of the most promising message encoding techniques is the CSK-method, because it utilizes relevant advantages of chaotic carriers. Firstly, the message is mixed by a nonlinear process into the chaotic carrier, providing a dynamical key inherent to the transmission of the message. Secondly, the message is spread over the bandwidth of the chaotic carrier reducing the sensitivity of the system to spectral perturbations. And thirdly, CSK can be easily applied via modulation of at least one of the system's parameters. Furthermore, for CSK the maximum transmission rate of the cryptosystem is only limited by the maximum carrier frequency.

In recent years, various approaches have been accomplished for the realization of chaos cryptosystems [11–14,17–20]. So far, research has mainly focused on synchronization properties of the systems proposed, i.e. synchronization quality, synchronization time, and message-carrier discrimination ratio. Meanwhile, a growing interest in the properties of chaotic carriers has emerged, since they affect functionality, applicability and security of chaos cryptosystems. For applications in high-speed data transmission-systems, for instance, where maximum bit-rates of multiple-Gbit/s and high reliability are desired, the maximum frequency and the bandwidth of the carrier should be as high as possible. Other characteristics of the carrier are relevant for the system's security, e.g. dimensionality, nonlinearity and autocorrelation properties [21–23]. Hence, for a successful implementation of a chaos cryptosystem all the performance aspects comprising carrier, encoding method, synchronization properties and decoding techniques have to be considered.

Semiconductor laser (SL) systems offer a particularly high potential for implementation in modern chaos cryptosystems. On the one hand, it is comparably easy to generate high-dimensional and broad-band chaotic emission dynamics with SLs which are subject to time delayed all-optical or electro-optical feedback [24–26]. On the other hand, SLs are standard elements in telecommunications. Thus, many of the optical and the electro-optical components required for an implementation in chaos cryptosystems are available. Furthermore, a utilization of existing fiber links seems to be accomplishable and of high value from an economical point of view.

So far, several chaos cryptosystems utilizing SLs subject to delayed feedback have been proposed, comprising different configurations and diverse encoding/decoding methods [18,19,27,28]. Some systems have been experimentally implemented and a proof of principle as cyroptosystems has been demonstrated [29–32]. In particular, SL-systems with optical feedback allow for the generation of the challenging dynamical and synchronization properties which are required. Furthermore, these systems are experimentally well-controllable and their dynamics are well-understood, since they have been intensively studied within the last two decades. So far, only SL-systems operating in the so called *long cavity regime* (LCR) have been considered and restricted attention has been paid to their properties if applied as carriers. The best carrier properties for the LCR have been found for moderate feedback and moderate pump-conditions, when the systems are operated in the fully developed coherence collapse [13]. However, the dynamics in the LCR reveal inherent limits regarding security and applicability. Two major disadvantages of the dynamics in the LCR are the long autocorrelation times, the restricted bandwidth and the residuals of system-inherent frequencies in the rf-spectra of the chaotic dynamics. As we will show, these and other restrictions can be overcome for systems with short delay times. For delay times comparable to the period of the relaxation oscillation frequency or shorter, the dynamical properties of the systems qualitatively change if compared to those of the LCR. Thus, a different dynamical regime is entered which is called the *short cavity regime* (SCR). In contrast to the LCR, in the SCR the dynamics of the systems strongly depend on the phase of the feedback. For low levels of pumping, a characteristic scenario comprising stable emission, regular pulse packages and chaotic dynamics can be observed when varying the phase of the feedback. This scenario has been characterized just recently [33,34].

The aim of this article is to emphasize the potential of SL-systems operating in the SCR for the realization of high-performance chaos cryptosystems. In Section 2, we discuss the generation of suitable chaotic carriers, generated by SLs which are subject to delayed optical feedback. We show that the performance and the privacy properties of the chaotic carriers can be significantly improved for systems operating in the SCR, if compared to systems operating in the LCR. These improvements are due to changes of the dynamical properties induced by a reduction of the delay time of the optical feedback down to a few hundred picoseconds. In the SCR, we are able to generate high-dimensional chaotic dynamics with almost flat rf-spectra extending to frequencies of up to multiple GHz. We analyze the influence of relevant system parameters on the dynamics and optimize the carrier. In Section 3, we demonstrate synchronization of a receiver system to this dynamics for the receiver being arranged in an open-loop configuration. For carefully adjusted conditions, we observe good synchronization properties and verify the properties which allow for successful message encryption/decryption. Motivated by the synchronization properties observed, we perform a digital signal transmission experiment which is discussed in Section 4. In the experiment, we encode a 500 MHz square wave signal via CSK so that it is not recognizable from the corresponding rf-spectrum. We demonstrate the capability of the synchronized receiver system for discriminating the signal and the carrier. Finally, we succeed in recovering the original signal by a simple extraction process.

2. Generation of carriers suitable for chaos cryptosystems

The generation of chaotic carriers exhibiting good carrier properties and evenmore being suitable for message encoding with GHz bandwidth is one of the fundamental requirements for building applicable chaos cryptosystems. In this section, we discuss the generation of chaotic carriers with SLs subject to delayed optical feedback which have proven to be promising systems to reach this goal.

2.1. Requirements for good carriers

In advance of the presentation of the experiments and the results, we define central requirements for chaotic carriers, which are summarized in Table 1. The requirements comprise physical and technical aspects accounting for functionality and applicability of the system. The physical requirements can be subdivided into two categories: performance and privacy. From the performance point of view, sufficient bandwidth, high maximum carrier frequency and good controllability of the key parameters are desirable. From the point of view of privacy, additional requirements need to be fulfilled. The most important ones are rapidly decreasing correlations of the dynamics, high information entropy and a suitable encoding method. In addition, the technical realization should be possible and feasible. Our aim is to generate a chaotic carrier which meets all of the requirements summarized in Table 1. One route to achieve this goal is sketched in the following section.

2.2. Semiconductor laser subject to delayed optical feedback

In this section, we introduce the chaotic carrier-generator of our choice, a SL subject to delayed optical feedback. A scheme of the experimental setup of the SL-system is depicted in Fig. 1. As a laser we use a HLP1400 Fabry–Perot semiconductor laser which is pumped by an ultra-low-noise DC-current source and whose temperature is controlled and stabilized to better

Table 1
Requirements for carriers suitable for chaos cryptosystems

	Physical	Technical
Performance	broad bandwidth well-controllable system parameters high carrier modulation index	robust well-controllable system parameters compact and cost-effective design
Privacy	broad bandwidth flat rf-spectrum rapidly decreasing correlation character of nonlinear function: strong stretching and folding chaotic attractor: numerous high-value Lyapunov exponents high information entropy suitable encoding technique selective on parameter tuning	

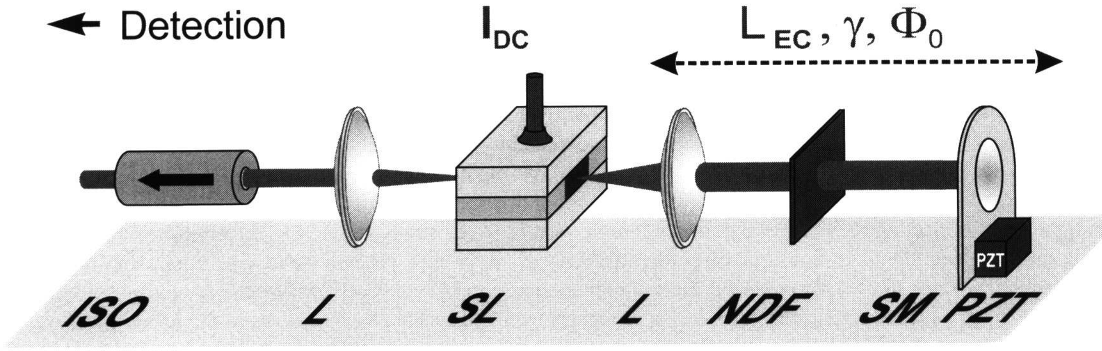

Fig. 1. Experimental setup of a semiconductor laser subject to delayed optical feedback.

than 0.01 K. The light emitted by the SL is collimated by a lens (L) and propagates towards a semitransparent mirror (SM) from which a part of the light is reflected back and reenters the laser after the time of flight, being $\tau = 2L_{EC}/c$, with the phase (difference) $\Phi_0 = \Phi(t) - \Phi(t - \tau)$. Here, L_{EC} stands for the length of the external cavity and c for the speed of light in air, while the ratio between the emitted power and the power of the feedback coupled into the laser is the feedback ratio γ. Such a SL-system is a delay system being, mathematically, infinite dimensional. The key parameters of the system determining the dynamical behavior are the delay time τ, the feedback ratio γ, the laser's pump current I_{DC} and the feedback phase Φ_0. These parameters can be varied by changing L_{EC}, by replacing the neutral density filter (NDF), by varying I_{DC} and by shifting the SM on sub-wavelength scale with a piezo-electric transducer (PZT), respectively. The light emitted from the rear facet of the laser is sent to the detection branch which is isolated (ISO) from the system in order to prevent unwanted back-reflections. One part of the light is detected by a 12 GHz photo detector, whose output is monitored on a 4 GHz bandwidth oscilloscope, and a rf-spectrum analyzer with 18 GHz bandwidth. The other part of the light is analyzed in an optical spectrum analyzer with a resolution of 50 pm.

A detailed analysis of the dynamics in dependence on the relevant system parameters of the SL-system operating in the LCR can be found in reference [24]. In the LCR the external cavity round-trip frequency $\nu_{EC} = 1/\tau$ is sufficiently smaller than the relaxation oscillation frequency of the laser which is a relevant frequency for the emission dynamics. Good carrier properties have been found for lasers with α-parameters of typically greater than 3 being the major nonlinearity in our system. Best operation conditions comprise moderate feedback and levels of pumping well above threshold. Under these conditions, fairly good dynamical properties can be found experimentally, i.e. chaotic dynamics with a maximum bandwidth in the GHz-range [24]. For comparable conditions, it has been shown in numerical modeling that the number (#) of positive Lyapunov exponents can exceed 100 [25] giving rise to high-dimensional chaotic dynamics. However, the bandwidth of the chaotic dynamics for systems with long external cavities is limited by the relaxation oscillation frequency of typically less than 10 GHz. Additionally, the carrier modulation index drops for frequencies between the external cavity resonance frequencies which restricts the carrier bandwidth and, hence, hinder broad-band message transmission. Furthermore, slowly decaying autocorrelation functions of the dynamics indicate unsuitably small information entropies for the carrier revealing a potential lack for the system's security [21–23].

In comparison to the LCR, the SCR allows for dynamics with frequencies exceeding 10 GHz significantly [33,34]. In this regime, dynamics with frequencies beyond the relaxation oscillation frequency can be realized. The limiting frequency for the bandwidth of SCR dynamics is ν_{EC} which can be sufficiently larger than the relaxation oscillation frequency. For even shorter cavities, the maximum frequency can be shifted to frequencies of several tens of GHz. However, a compromise concerning maximum bandwidth and entropy of the dynamics has to be made, since the entropy of the dynamics decreases for reducing L_{EC} too far, which has been verified from numerical modeling [35]. So far, the dynamical phenomena which have been reported in the SCR comprised regular, quasi-periodic or low dimensional chaotic dynamics which are not suited for application in chaos cryptosystems. In the following section we demonstrate that, for adjusted system parameters, the SCR can be utilized for the generation of chaotic dynamics meeting all the properties required for high-performance chaos cryptosystems.

2.3. *Carrier properties in the short cavity regime*

In the experiments, we have investigated the influence of the pump level I_{DC}, the feedback ratio γ, the cavity length L_{EC} and the feedback phase Φ_0 on the emission dynamics of the system. We note that in the SCR special care has to be taken for the stability of the system, in particular for the adjustment of the feedback phase Φ_0, since the dynamics strongly depend on this parameter [33,34]. This is in contrast to the behavior of the dynamics in the LCR, where the dynamics are almost independent

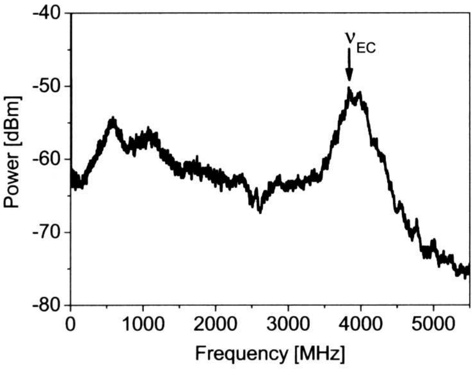

Fig. 2. rf-spectrum of the emission dynamics for a SL-system operating in the SCR. The length of the external cavity is 3.9 cm and the pump level is $I_{DC} = 1.2I_{th}$. The feedback ratio γ is 4.8%.

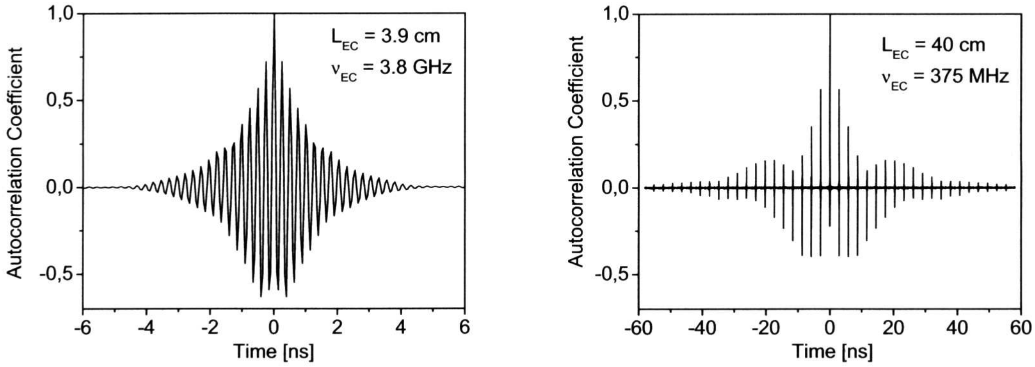

Fig. 3. Autocorrelation function of the SL-system operating in the SCR. The parameters are: $L_{EC} = 3.9$ cm, $I_{DC} = 1.2I_{th}$ and $\gamma = 4.8\%$.

Fig. 4. Autocorrelation function of the SL-system operating in the LCR. Except the length of the external cavity, which is $L_{EC} = 40$ cm, the conditions are similar to those of Fig. 2 and Fig. 3.

on small variation of Φ_0. In the LCR, an influence of a change of Φ_0 on the dynamics can only be revealed by application of detection techniques utilizing synchronization phenomena [36].

Here, we have chosen the length of the external cavity to be 3.9 cm, corresponding to a round-trip frequency of $\nu_{EC} = 3.8$ GHz. This length has been chosen to allow for the resolution of the external cavity frequency with the oscilloscope, having an analog bandwidth of 4 GHz. Furthermore, we have chosen a moderate feedback ratio of $\gamma = 4.8\%$. We note that for these conditions and for pumping near the solitary laser threshold current I_{th} we find the typical SCR dynamics, as they have been reported in [33,34]. In the following experiments, the DC-injection current I_{DC} of the laser was chosen to be 20% above I_{th}. For this pump level the relaxation oscillation frequency of the solitary laser has been determined to be $\nu_{RO} \approx 2.3$ GHz. We are able to obtain broad-band chaotic dynamics for carefully adjusted feedback phase Φ_0, while results of corresponding numerical modeling verify that high-dimensionality (~ 10) is maintained [35]. The rf-spectrum of the corresponding chaotic dynamics is depicted in Fig. 2. The spectrum reveals the high bandwidth of the dynamics. It does not exhibit characteristic frequencies except for the broad peak close to the external cavity round-trip frequency ν_{EC} which is marked in the figure. The bandwidth comprises frequencies even exceeding ν_{EC} by a few hundred MHz revealing a steep fall-off for higher frequencies. We find a continuous and flat rf-spectrum in the range from a few hundred MHz up to the external cavity round-trip frequency ν_{EC}. The corresponding range in these experiments is approximately 3 GHz. We note that this range can be extended to frequencies significantly exceeding 10 GHz without loosing the flatness of the rf-spectrum. This is simply done by reducing the delay time τ and, therefore, shifting ν_{EC} to higher frequencies, which is accompanied by an increasing bandwidth of the dynamics [33]. However, detection becomes more challenging for increasing bandwidth.

An important issue related to security is the correlation properties of the dynamics. The autocorrelation functions of the intensity dynamics of the delay system for both, SCR and LCR, are depicted in Figs. 3 and 4, respectively. At this point, we note that the details of the autocorrelation function for the SCR-dynamics are not fully resolved, since the analog bandwidth of the oscilloscope is limited to 4 GHz, which is slightly less than the bandwidth of the corresponding dynamics. A comparison of

Table 2
Physical properties of the carrier generated by the SCR-SL-system for the same conditions as for the rf-spectra presented in Fig. 2

	Physical
Performance	bandwidth: up to ν_{EC} (multiple GHz) well-controllable parameters carrier modulation-index: 20 dB for ν_{mod} up to 2.5 GHz...
Privacy	bandwidth: DC to ν_{EC} ($\nu_{\mathrm{EC}} \gg \nu_{\mathrm{RO}}$) broad, almost flat rf-spectrum short correlation: $< 4\,\tau_{\mathrm{EC}}$ (< 1 ns) strong nonlinearity $\alpha \approx 3$ $\#(\lambda > 0) \approx 10$ sufficiently high entropy encryption methods: CSK, CM, CMK selective on parameter tuning

the correlation properties reveals a suspiciously faster fall-off of the correlations in the SCR than in the LCR while a sufficiently high information entropy is maintained [35]. This property emphasizes the high potential of the SCR-dynamics for encrypted data transmission, since a decay of the correlation function within a few ns corresponding to just a few cycles of the light in the external cavity prevents successful application of embedding-techniques for phase-space reconstruction of the chaotic attractor [21–23].

In comparison with the requirements defined in Table 1, we summarize the properties of the dynamics for this configuration in Table 2. It becomes clear from the table, that the privacy-properties are complemented by good performance-properties. These are sufficient signal/noise ratio, carrier modulation-index, selectivity on parameter tuning and robustness against environmental influence. Furthermore, the carrier-generator can be implemented in a compact and cost-effective design of a chaos cryptosystem. In summary, the requirements on the carrier-generator defined in Table 1 have been fulfilled.

3. Chaos synchronization of short cavity carriers

The principle of chaos cryptosystems is based on chaos synchronization phenomena. Therefore, the structure of a receiver system has to be matched to that of the transmitter and might be unique for the chosen transmitter system.

In the following experiments, a receiver system in an open-loop configuration has been studied, since it is, due to its simplicity, a good model configuration for chaos synchronization experiments. Additionally, the configuration has proven to be robust and could be easily implemented in a chaos cryptosystem.

3.1. Open-loop configuration

In the open-loop configuration, the receiver system consists of a solitary laser without feedback. Fig. 5 depicts the experimental setup with the transmitter and the receiver subsystems. Since well-matched parameters are essential for synchronization experiments, we have selected two device-identical SLs (uncoated Hitachi HLP1400 Fabry–Perot SLs) from the same wafer. Their optical spectra agree within 0.1 nm, their slope-efficiency within 3% and their threshold currents within 7%. Each laser is pumped by a low-noise DC-current source, and temperature stabilized to better than 0.01 K. The two sub-systems are optically coupled via the injection of a well-defined fraction of the optical field of the transmitter system into the receiver laser. The double stage optical isolator and the polarizer guarantee unidirectional coupling via the dominant TE component of the field. The strength of the coupling can be adjusted by placing a neutral density filter (NDF) between the transmitter and the receiver system. In the experiments both lasers were operated at $I_{\mathrm{DC}} = 1.2 I_{\mathrm{th}}$, for which the relaxation oscillation frequencies amount to $\nu_{\mathrm{RO}} \approx 2.3$ GHz. The length of the transmitter's external cavity was chosen to be 3.9 cm corresponding to a round trip frequency of 3.8 GHz. The coupling strength to the receiver has been optimized to achieve best possible synchronization of the receiver to the carrier generated by the transmitter. Optimal conditions have been found when the threshold reduction of the transmitter due to the feedback was 6% of I_{th}, whereas the threshold reduction for the receiver induced by the injection from the transmitter was 4% of I_{th}.

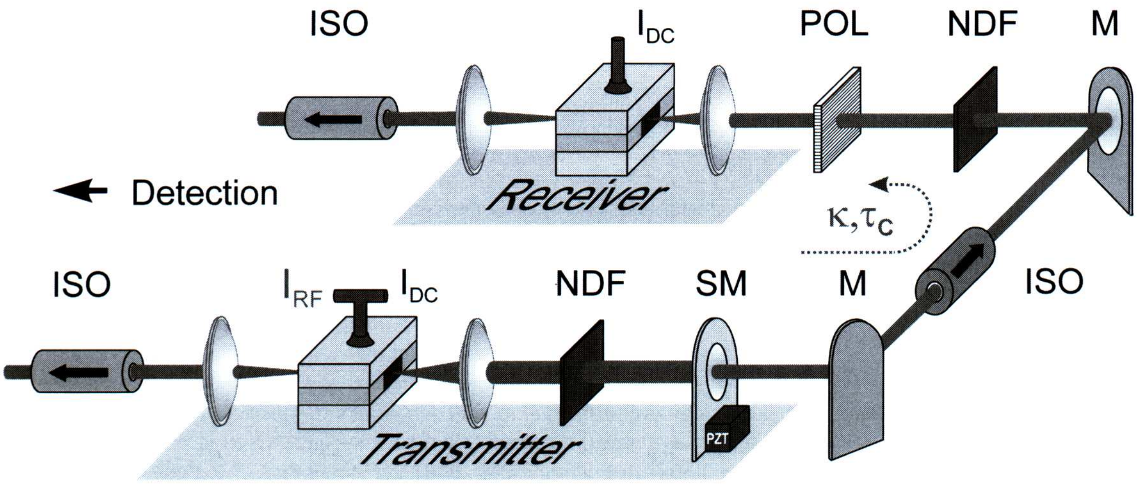

Fig. 5. Experimental setup of two unidirectionally coupled semiconductor laser systems in an open-loop configuration.

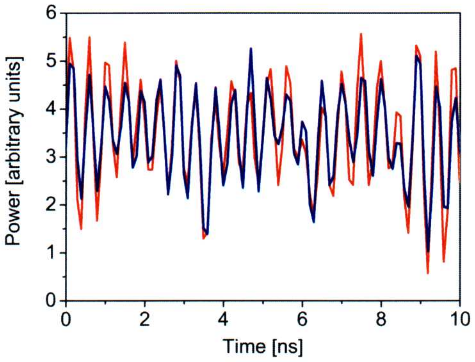

Fig. 6. Segments of the chaotic emission dynamics of the transmitter and the receiver in case of synchronization. The time series of the receiver has been shifted forward by the coupling time of $\tau_c = 6.6$ ns.

3.2. Synchronization properties

We are able to synchronize the chaotic SCR-dynamics of the two lasers and find cross correlation coefficients of up to 0.8 for optimized conditions. Under these conditions, the rf-spectra of the intensity dynamics of the lasers reflect the well-suited dynamical properties which have been discussed in Section 2.3. The rf-spectra are in excellent agreement in a broad range of frequencies up to ν_{EC}, demonstrating the good synchronization quality. In order to reveal the excellent synchronization of the dynamics even on sub-ns timescales, a 10 ns long window of the corresponding emission dynamics is presented in Fig. 6. In the figure, the transmitter's time series is represented in red color whereas the one of the receiver is depicted in blue color. The time series of the receiver has been shifted forward in time in order to facilitate comparison, because the receiver dynamics lags by the coupling time τ_c.

In order to verify whether the synchronization properties are suitable for a chaos cryptosystem, we test the configuration for Chaos-Pass-Filter (CPF) properties. CPF means that the synchronized receiver laser reproduces the chaotic oscillations but suppresses an external perturbation applied to the transmitter. This process is linked to the existence of a stable synchronization manifold and is an intrinsically nonlinear process. Hence, if the configuration exhibits CPF-properties, we can conclude that synchronization is stable. Vice versa, a stable synchronization manifold implies CPF-properties which allow for discrimination of the message, which plays the role of a perturbation, and the carrier in the synchronized receiver system. This is exactly the principle utilized for message extraction in our chaos cryptosystem.

In the experiment, we have applied the message in form of a small AC-current-modulation I_{RF} which has been added to the transmitter's DC-current I_{DC}. We emphasize that adding a message in this way does not give rise to a detectable intensity variation of the output at the modulation frequency. The message is indeed mixed nonlinearly within the carrier and not just hidden in it. The amplitude of the modulation has been chosen to be 1% of I_{th}. Thus, the perturbation is small enough to prevent changes of the spectral properties of the transmitter's dynamics, except changes introduced at the modulation frequency. We monitor the effect of the perturbation on the synchronized receiver dynamics. The rf-spectra of both of the lasers still agree very well, except for the modulation frequency. At this frequency, we measure distinct less power for the message in the receiver system than for the message in the transmitter system. Thus, the corresponding ratio between the power of the message in the transmitter and that measured in the receiver reflects the CPF-properties. This ratio is called message/carrier discrimination-ratio.

In order to characterize the frequency characteristics of the message/carrier discrimination-ratio which determine the possible bandwidth for message transmission, we have performed measurements of the signal suppression of the receiver over the full bandwidth of the intensity dynamics of the system. We achieve moderate suppression values of at least 10 dB in a broad range of frequencies up to about 2.5 GHz with a maximum of 22 dB. From these results, we conclude the existence of a synchronization manifold for the open-loop configuration exhibiting good stability properties. Furthermore, reasonable suppression between 10 dB and 5 dB can be obtained even up to the cavity round trip frequency which is significantly beyond the relaxation oscillation frequency of the solitary laser of approximately 2.3 GHz. However, there are some variations in the frequency characteristics of the suppression ratio even for small modulation amplitudes. Consequently, the question arises if these characteristics of this nonlinear filter process prevent or deteriorate the message extraction process. The answer to this question will be given in the following section. In Section 4, we study the possibility of a joint integration of both properties the well-suited carrier properties, obtained for SCR-dynamics, and the good synchronization properties of the open-loop configuration into a chaos cryptosystem.

4. Short cavity chaos cryptosystem

In the previous section, we have reported good CPF-properties for the open-loop configuration with high message/carrier discrimination-ratios in a broad range of frequencies. These properties are a major requirement for broad-band transmission utilizing chaotic carriers. The definition of a good encoding/decoding method for GHz-messages is not only closely linked to the encoding properties of the carrier, but also to the decoding properties of the receiver with respect to the applied encoding method.

Based on the successful synchronization in the open-loop configuration, in conjunction with its good CPF-properties, we have performed digital signal transmission experiments for the CSK encoding method via direct current modulation of the transmitter laser. The challenge of utilizing this method in the chosen dynamical regime lies in the continuous rf-spectrum, avoiding conspicuous resonances which can deteriorate the efficiency of the message encryption. Furthermore, the signal modulation has to be chosen so weak that no fingerprints can be seen in the rf-spectrum. An optimum nonlinear mixing of the message into the dynamics is desired. In order to meet the requirements of more realistic modulation signals, we have used square wave (SQW) signals as model messages. We use the term 'more realistic' since the physically relevant steep slopes for digital information encoding can be studied by using SQW-signals. Furthermore, they allow for analysis of the influence of nonlinearities in the extraction process. We note that an extension to random bit-pattern messages is required for a characterization of the system in terms of Bit-Error-Rate (BER), however, this is beyond the scope of this manuscript. The physics of message encryption/decryption can be studied well by applying SQW-signals, providing more information than the harmonic test signals we have analyzed in the previous section. We have chosen the amplitude of the SQW-signal such that it cannot be recognized from the rf-spectra. The corresponding rf-spectra of the transmitter and the receiver laser are depicted in Fig. 7. The rf-spectra show excellent agreement, indicating the good synchronization properties of the receiver.

The fundamental modulation frequency ν_f is located at 500 MHz, and the amplitude of the modulation current is 0.3% of I_{th}. The main question is, if and how the digital signal, which has been mixed nonlinearly within the carrier, can be extracted again. Demanding processing should be avoided since it would increase the complexity and the potential costs of such a system significantly. A good compromise between simple realization and good message/carrier discrimination has to be found. Therefore, we have performed an extraction process based on the following procedure:

(i) Subtract the mean of the transmitter- and the receiver output;
(ii) Normalize the variance of the receiver signal to the variance of the transmitter signal;
(iii) Subtract the normalized receiver signal from the normalized transmitter signal;
(iv) Filter the resulting signal with a multi-bandpass filter ($\nu \times 0.5$ GHz ± 0.15 GHz);
(v) Smooth the extracted message by low-pass filtering (2 GHz cut-off frequency).

We demonstrate that although no indications of the modulation can be captured from the rf-spectra, successful extraction of the signal is still possible. This is illustrated in Fig. 8, depicting a 10 ns long segment of the intensity dynamics of the transmitter (red) and the receiver (blue). The original SQW-signal is presented as green solid line at the bottom of the figure, while the

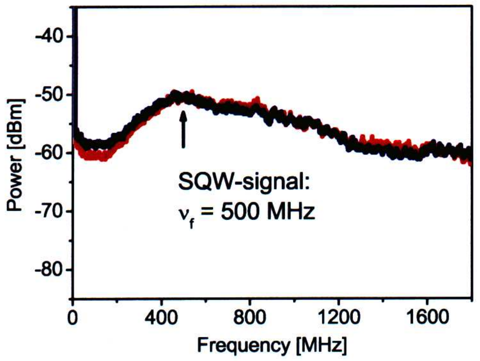

Fig. 7. rf-spectra of the transmitter and the receiver laser for a square wave modulation at a fundamental frequency of $\nu_f = 500$ MHz. The spectrum of the transmitter is depicted in red and that of the receiver in blue.

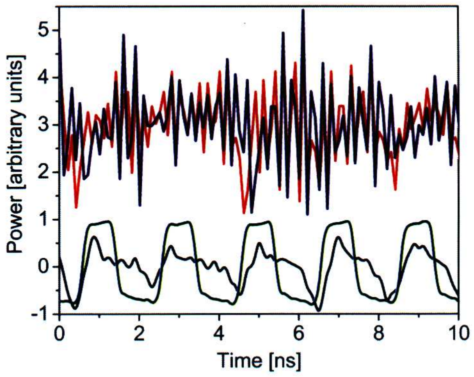

Fig. 8. Corresponding segments of the intensity time series of the transmitter and the receiver laser. The time series of the transmitter is depicted in red color and that of the receiver in blue color. The original modulation SQW-signal is represented by the green line, while the extracted signal from the receiver is depicted as black line.

corresponding extracted signal, which has been obtained following the procedure above, is presented as black solid line. We find that the extracted signal is distorted. These distortions originate from the nonlinear characteristics of the CPF-properties and are not due to insufficient averaging. Nevertheless, signal extraction of the digital signal from the receiver remains possible, in particular when considering the sensitivity of our extraction process to the rising edges of the signal. We note that in our experiment the maximum modulation frequency was limited to 500 MHz by the pulse generator. We expect that an extension of the message frequency into the GHz-range and to arbitrary bit-patterns is possible since the results obtained in Section 3.2 demonstrated suitable CPF properties up to several GHz. How far the distortions of the extracted signal are related to the synchronization process for the open-loop configuration needs to be clarified in further experiments. The corresponding results are expected to allow for an improvement of the encoding and decoding method, which could reduce the message distortions.

Finally, we note that it is not straightforward that the difference-signal extraction-process is a good choice in this configuration for the following reason. The type of synchronization chosen in these experiments for means of robustness is the generalized synchronization. Differences between perfect and generalized synchronization have been highlighted in [37]. The main point of concern is that generalized synchronization means that transmitter and receiver do not exhibit identical signals even for best synchronization performances. These deviations have to be quantified in terms of BER for applications in real transmission-systems. Furthermore, it remains to be verified that transmission of real digital messages with multiple-Gbit/s rates is possible, even for distances exceeding several kilometers.

5. Conclusions

In conclusion, we have demonstrated that SLs subject to delayed optical feedback operating in the *short carrier regime* (SCR) are well-suited generators of chaotic carriers for modern chaos cryptosystems. First, we have analyzed the emission dynamics of a SL with delayed optical feedback with respect to privacy and performance aspects. We found that a significant enhancement of the dynamical properties can be achieved for systems operating in the SCR, if compared to those of systems operating in the *long cavity regime*. We were able to generate high-dimensional chaotic dynamics comprising excellent spectral properties and an enhanced bandwidth of around 4 GHz. The good dynamical properties and the enhancement in the bandwidth of the carriers, which is due to dynamical properties being characteristic for the SCR, offer a high potential for an implementation as carrier-generators in encrypted multi-Gbit/s chaos cryptosystems. Motivated by this prospect, we performed synchronization experiments in an open-loop configuration under these conditions. We succeeded in synchronizing the chaotic transmitter and receiver dynamics and found well-suited synchronization properties. Furthermore, we verified good Chaos-Pass-Filter properties of up to 20 dB suppression in a broad range of frequencies, being essential for message extraction in chaos cryptosystems. Finally, we have coalesced all these aspects and studied the potential of the configuration for encrypted message transmission. In the first step, we have successfully encrypted a digital 500 MHz square wave signal into the carrier via a CSK-scheme, realized by adding an AC-current modulation to the transmitter. The encoded digital signal has been transmitted to the synchronized receiver system and we succeeded in decoding the encoded signal by applying a simple substraction process.

The chaos cryptosystem presented in this work utilizes the good carrier properties which have been found in the SCR. Based on the excellent properties, we were able to demonstrate a functional cryptosystem, unifying widespread demands on applicability and privacy.

Acknowledgements

We acknowledge financial support by the European Commission within the project: OCCULT – Optical Chaos Communication Using Laser-diode Transmitters. IST-2000-29683.

References

[1] L.M. Pecora, T.L. Carroll, Phys. Rev. Lett. 64 (1990) 821.
[2] H.G. Winful, L. Rahman, Phys. Rev. Lett. 65 (1990) 1575.
[3] M.G. Rosenblum, A.S. Pikovsky, J. Kurths, Phys. Rev. Lett. 78 (1997) 4193.
[4] T. Sugawara, M. Tachikawa, T. Tsukamoto, T. Shimizu, Phys. Rev. Lett. 72 (1994) 3502.
[5] R. Roy, K.S. Thornburg Jr., Phys. Rev. Lett. 72 (1994) 2009.
[6] K. Coffman, W.D. Mc Cormick, H.L. Swinney, Phys. Rev. Lett. 56 (1986) 999.
[7] S.H. Strogatz, I. Stewart, Sci. Am. 269 (12) (1993) 68.
[8] C. Schäfer, M.G. Rosenblum, J. Kurths, H.H. Abel, Nature 392 (1998) 239.
[9] L. Glass, Nature 410 (2001) 277.
[10] F. Hoppenstaedt, E.M. Izhikevich, Phys. Rev. E 62 (2000) 4010.
[11] G.D. VanWiggeren, R. Roy, Phys. Rev. Lett. 81 (1998) 3547.
[12] K. Cuomo, A.V. Oppenheim, Phys. Rev. Lett. 71 (1993) 65.
[13] I. Fischer, Y. Liu, P. Davis, Phys. Rev. A 62 (2000) 011801(R).
[14] G.D. VanWiggeren, R. Roy, Phys. Rev. Lett. 88 (2002) 097903.
[15] F. Dachselt, W. Schwarz, IEEE Trans. Circuits Syst. I 48 (2001) 1498.
[16] C.R. Mirasso, J. Mulet, C. Masoller, IEEE Photon. Technol. Lett. 14 (2002) 456.
[17] V. Annovazzi-Lodi, S. Donati, A. Sciré, IEEE J. Quantum Electron. QE-32 (1996) 953.
[18] L. Larger, J.-P. Goedgebuer, F. Delorme, Phys. Rev. E 57 (1998) 6618.
[19] T. Heil, J. Mulet, I. Fischer, C.R. Mirasso, M. Peil, P. Colet, W. Elsäßer, IEEE J. Quantum Electron. QE-38 (2002) 1162.
[20] A. Uchida, S. Yoshimori, M. Shinozuka, T. Ogawa, F. Kannari, Opt. Lett. 26 (2001) 866.
[21] K.M. Short, A.T. Parker, Phys. Rev. E 58 (1998) 1159.
[22] J.B. Geddes, K.M. Short, K. Black, Phys. Rev. Lett. 83 (1999) 5389.
[23] V.S. Udaltsov, J.-P. Goedgebuer, L. Larger, J.B. Cuenot, P. Levy, W.T. Rhodes, Phys. Lett. A 308 (2003) 54.
[24] I. Fischer, T. Heil, W. Elsäßer, in: B. Krauskopf, D. Lenstra (Eds.), Fundamental Issues of Nonlinear Laser Dynamics, Melville, New York, AIP Conf. Proc. 548 (2000) 218.
[25] V. Ahlers, U. Parlitz, W. Lauterborn, Phys. Rev. E 58 (1998) 7208.
[26] J.-P. Goedgebuer, P. Levy, L. Larger, C.-C. Chen, W.T. Rhodes, IEEE J. Quantum Electron. QE-38 (2002) 1178.
[27] C.R. Mirasso, P. Colet, P. Garcia-Fernandez, IEEE Photon. Technol. Lett. 8 (1996) 299.
[28] D. Kanakidis, A. Argyris, D. Syvridis, IEEE J. Lightw. Technol. 21 (2003) 750.
[29] S. Sivaprakasam, K.A. Shore, IEEE J. Quantum Electron. QE-36 (2000) 35.
[30] J.-M. Liu, H.-F. How-foo Chen, S. Tang, IEEE J. Quantum Electron. QE-38 (2002) 1184.
[31] J. Ohtsubo, IEEE J. Quantum Electron. QE-38 (2002) 1141.
[32] M.W. Lee, L. Larger, J.-P. Goedgebuer, IEEE J. Quantum Electron. QE-39 (2003) 931.
[33] T. Heil, I. Fischer, W. Elsäßer, A. Gavrielides, Phys. Rev. Lett. 87 (2001) 243901.
[34] T. Heil, I. Fischer, W. Elsäßer, B. Krauskopf, K. Green, A. Gavrielides, Phys. Rev. E 67 (2003) 066214.
[35] R. Vicente, J. Daudén, P. Colet, R. Toral, in: Physics and Simulation of Optoelectronic Devices XI, SPIE Proceedings, 2003.
[36] M. Peil, T. Heil, I. Fischer, W. Elsäßer, Phys. Rev. Lett. 88 (2002) 174101.
[37] R. Vicente, T. Pérez, C.R. Mirasso, IEEE J. Quantum Electron. QE-38 (2002) 1197.