Synchronization of Chaotic Lasers by Optical Feedback for Cryptographic Applications
Valerio Annovazzi-Lodi, Member, IEEE, Silvano Donati, Member, IEEE, and Alessandro Scirè

Abstract—We propose a new scheme for synchronization of the optical chaos generated by a semiconductor laser subjected to external reflection. The scheme is based on optical feedback and will be analyzed from the viewpoint of static and dynamic properties and of robustness to external perturbations and noise. An application to cryptographic communications (chaotic shift keying) is finally proposed.

Index Terms—Chaos, cryptography, laser, laser stability.

I. INTRODUCTION

THE CHAOTIC regime [1] is the well-known behavior of a large class of nonlinear systems and consists of pseudorandom oscillations, which are reproducible only when starting from identical initial conditions and parameter values. Many chaotic systems have been demonstrated in the field of optics. For example, it has been widely shown that a semiconductor laser may be routed to chaos by injection from another source [2] or simply by backreflection from an external mirror [3]. Recently, chaos has been proposed for a number of applications in the telecommunications field. Among them, cryptographic communication is especially attractive since it fully exploits the characteristic of chaos of being deterministic, showing, at the same time, a strong dependence on even minimal variations of initial conditions and parameter values.

Chaotic cryptography [4], [5] usually relies on a couple of systems which generate the same chaotic waveform, one of which is used to hide information at the transmitter, and the other to recover data at the receiver. Many authors have dealt with synchronization of chaos, finding methods to force two chaotic systems on the same trajectory in the phase plane [6]–[10], in spite of environmental disturbances and/or small parameter mismatch.

In a previous paper [4], we demonstrated the robustness of the Kapitaniak’s [11], [12] synchronization method applied to a chaotic system composed of two semiconductor lasers, one of which was driven to chaos by injection from the other [2], and demonstrated its application to different cryptographic schemes. In the present paper, we propose a similar approach using a single laser diode with backreflection as the basic chaotic system. Both schemes are all-optical and share the same inherently high speed and wide spectrum spreading; however, the new one is easier to implement and requires half the number of laser sources.

II. SYNCHRONIZATION SCHEME

The basic chaotic system is shown in Fig. 1(a) and consists of a semiconductor laser with an external mirror and an attenuator. Let us introduce the field transmission $K$ which accounts for all losses in the two-way path between the laser and the mirror. Thus, parameter $K$ includes not only the loss from the attenuator $H$, but also attenuation due to misalignment of the external mirror, as well as to partial transmission of the laser output mirror and of the splitter for the input $A$ (which will be used to inject the synchronizing signal).

This system has been shown to route to chaos [3], following a period duplication sequence with order parameter $K$.

To synchronize two such systems, we propose the block diagram shown in Fig. 1(b), where both $S1$ and $S2$ have the topology of Fig. 1(a).

Let us assume, for the moment, that $S1$ and $S2$ share the same nominal values of all parameters (twin systems). As it is well known, even twin systems would follow completely different trajectories if they start from slightly different initial conditions and are isolated from each other.

By definition, synchronization means that $|E_2 - E_1| \to 0$ for $t \to \infty$; in practice, the output fields $E_{1f}, E_{2f}$ of $S1$ and $S2$
are expected to become virtually coincident after a sufficiently long time of interaction.

In the master–slave configuration of Fig. 1(b), $E_2$ is subtracted from $E_1$ and the difference feeds the input port $A_2$ of $S_2$. When the output fields are identical, $S_2$ is virtually isolated from $S_1$, because the total injected field into port $A_2$ vanishes. However, if a perturbation causes $E_2 \neq E_1$, then an error signal $E_2 - E_1$ arises at port $A_2$ and contributes to injection until system $S_2$ (the slave) synchronizes again to $S_1$ (the master).

The scheme of Fig. 1(b) has been analyzed by numerical simulations, as detailed below. We describe systems $S_1$ and $S_2$ in terms of slowly varying field amplitudes and phases $E_i, \phi_i$ using the well-known Lang–Kobayashi equation set [13], i.e.,

$$\frac{dE_i}{dt} = \frac{1}{2} \left\{ G_n(N_i - N_0)(1 - \epsilon \Gamma E_i^2) - \frac{1}{\tau_p} \right\} E_i + \frac{K}{\tau_m} E_{\text{in}}(t) \cos[\phi_i(t) - \phi_{\text{in}}(t)] \quad (1a)$$

$$\frac{d\phi_i}{dt} = \frac{1}{2\epsilon^*} \left\{ G_n(N_i - N_0)(1 - \epsilon \Gamma E_i^2) - \frac{1}{\tau_p} \right\} - \frac{K}{\tau_m \epsilon} E_i(t) \sin[\phi_i(t) - \phi_{\text{in}}(t)] \quad (1b)$$

$$\frac{dN_i}{dt} = \frac{1}{\tau_p} E_i(t) - \frac{N_i}{\tau_R} - G_n(N_i - N_0)(1 - \epsilon \Gamma E_i^2)E_i^2 \quad (1c)$$

where $i = 1, 2$ for $S_1, S_2$. From Fig. 1(a), the forcing term of $S_1$ is the field reflected by the mirror (delayed by the time of flight $\tau_{\text{ext}}$), whose amplitude and phase are

$$E_{\text{in}} = E_1(t - \tau_{\text{ext}}) \quad (2a)$$

$$\phi_{\text{in}} = \phi_1(t - \tau_{\text{ext}}) - \omega_0 \tau_{\text{ext}} \quad (2b)$$

From Fig. 1(b), the forcing term of $S_2$ is the total injected field

$$E_2 \exp^{j \phi_2} = E_2(t - \tau_{\text{ext}}) \exp\{j[\phi_2(t - \tau_{\text{ext}}) - \omega_0 \tau_{\text{ext}}]\} + E_1(t) \exp^{j \phi_1(t)} - E_2(t) \exp^{j \phi_2(t)} \quad (3)$$

and includes, in addition to the mirror reflection, injection contributions from both $S_1$ and $S_2$. For the moment, we neglect the delay in the feedback path $C$, which will be considered later.

The meaning of the other parameters in (1)–(3) is standard in literature [4], [13] and is reported in Table I, along with the values used in the numerical simulation, which represent a generally accepted set for a semiconductor laser of 1 mW power output [2]. As it is customary, in the following, we will use the normalized current $J_0 = J/J_{\text{th}} = R_p/R_{p\text{th}}$ as the pump parameter (the subscript “th” refers to values at the laser threshold).

We have first analyzed the synchronization of $S_1$ and $S_2$ by considering identical systems with different starting conditions.

We have found that, in the whole range of parameters $K$ and $R_p$ reported in Table I, the twin systems synchronize after a short transient (20–30 ns, typically). Fig. 2 shows, in a typical case, the evolution of the synchronization error, defined as the difference between fields $E_2$ and $E_1$, normalized to the unperturbed value $E_0$ of the output field, i.e., $(E_2 - E_1)/E_0$.

From this diagram, it can be seen that, strictly speaking, a perfect synchronization is never reached, because, even for twin systems, $E_2 - E_1$ does not vanish but settles on a small zero-mean fluctuation. Thus, to express quantitatively in the following the degree of synchronization, we introduce the mean relative error

$$\sigma_s = \langle |E_2 - E_1| \rangle / E_0 \quad (4)$$

Among parameters describing the twin systems, two of them, which allow easy and fast control by the user, will be referred to as “external parameters” in the following. They are the transmission $K$ and the pump level $J_0$. All others parameters in Table I will be called “internal.”

Since external parameters can be easily modified, we have looked for their optimum values, i.e., those leading to short transients and low steady-state error $\sigma_s$. For nominal values of the internal parameters, we have obtained the results of Fig. 3 and then we have chosen $J_0' = 1.3$ and $K' = 7.74 \times 10^{-4}$ as the optimum set for both $S_1$ and $S_2$, at the center of a rather wide region where the error is small ($\sigma_s < 10^{-4}$) and slowly

![Table I](image-url)
Fig. 3. Mean synchronization error $\sigma_s$ versus external parameters $K$ and $J_0$.

varying. Around this setpoint, Fig. 4(a) shows the error $\sigma_s$ as a function of external parameter mismatch.

The situation is different for internal parameters, which cannot be perfectly matched in two real lasers. Thus, for the optimum set $(K^*, J_0^*)$ we have evaluated the error $\sigma_s$ as a function of the relative mismatch of the internal parameters. The result is shown in Fig. 4(b) (full line) and has been calculated by changing all values at the same time. It is found that $\sigma_s$ is kept below 0.01 as long as mismatch is less than 5%.

An important supplementary result is that the adjustment of the external parameters provides a way to compensate for the effect of internal parameter mismatch. As an illustration of this point, Fig. 4(b) shows the typical improvement (dotted line) obtained by slightly modifying $K$ and $J_0$ of the slave system $S_2$ from their nominally optimum values.

**III. SYNCHRONIZATION AND NOISE**

Let us now evaluate the sensitivity of the synchronization error to perturbations and noise. Since the approach is based on negative feedback, we expect that, when a disturbance drives the two lasers on different trajectories, the system is able to correct its regime and synchronize again.

Indeed, this is what has been found from simulations. As regard to disturbances, we have considered pulse fluctuations acting on the pump. As regard to noise, we have assumed a generic additive white Gaussian process superposed on fields $E_1$ and $E_2$. Referring to (1), this amounts to add to both components of each field, namely, $E_{i\alpha}$ and $E_{i\beta}$ ($i = 1, 2$), a random fluctuation $\xi_{i\alpha}$ or $\xi_{i\beta}$ with zero mean and variance $\sigma^2$.

In both cases, we have been able to conclude that the scheme of Fig. 1(b) provides good rejection to disturbances. This can be appreciated from Fig. 5, showing a transient after a short pulse ($0.2J_0$ for 2 ns) on the pump, and from Fig. 6, where we report the synchronization error from white additive noise, for $\sigma$ spanning from 0 to $0.1E_0$. Such noise level is much larger than the shot noise and allows to model a rather strongly disturbed interconnection. For this reason, and to simplify the numerical analysis, we have selected this approach, instead of integrating the Langevin equations.

Also, we have analyzed the effect of filtered noise; as expected, we have found that the spectral components which more strongly perturb synchronization are those next to the chaotic signal central frequency (which is close to the laser relaxation frequency). On the other hand, noise effects rapidly decrease moving away from the central frequency (1 GHz in our case), i.e., over 4–5 GHz and under 100 MHz with our set of parameters.

Recently [5], a scheme has been presented, which works by injecting a fraction $T$ of the output field of $S_1$ into $S_2$, and is appealing because it is very simple to implement.
However, from numerical simulations, we have found that its static and dynamic performances are not as good as with the scheme of Fig. 1(b). More specifically, the synchronization error $\sigma_s$ depends on a larger extent on external parameters $K, \sigma_0$, and $T$. Using the same parameter values as in [5] ($K = 7 \times 10^{-1}, T = 10^{-3}, J_0 = 2.99$), we get $\sigma_s \sim 0.01$, but the synchronization error increases markedly when moving apart from this set point, as it is shown in Fig. 4(b) by the dashed-dotted line. Also, the system reacts less quickly to external disturbances, and after applying a small perturbation it does synchronize again, but the transient is markedly longer than with the scheme of Fig. 1(b). All of the above limitations can be readily explained by the lack of a feedback path, which instead has been included in our system.

IV. CRYPTOGRAPHY

Using the proposed synchronization method, we have simulated a chaotic shift keying (CSK) transmission [4] based on parameter coding. The block scheme is shown in Fig. 7. The information is entered in $S_1$ by assigning the two symbols “0” and “1” to different transmission values $K_0$ and $K_1$, which correspond to different orbits of the same chaotic attractor. This can be implemented, e.g., by a switch or a modulator placed between the laser and the mirror and fed by the bit string to be transmitted.

Thus, system $S_1$ generates a modulated chaotic waveform hiding the bit sequence. Due to the properties of chaotic waveforms, much as in [4], information cannot be recovered by an eavesdropper using conventional methods (including spectrum scanning or correlation techniques). Also, it would be impractical to store the waveform for off-line processing because its spectrum is very wide (more than 10 GHz), and even the bit rate cannot be extracted by observing the transmitted waveform in the frequency or time domains. Finally, due to the pseudorandom nature of the chaotic waveform, there is no correlation between two equal sequences transmitted at different times.

However, the authorized listener, who knows system parameters, can recover information by synchronization.

To this purpose, at the receiver (Fig. 7), the signal is sent to two chaotic systems ($R_1$ and $R_2$), identical to that at the transmitter, one of which is tuned on the $K$ value corresponding to “1” and the other on that corresponding to “0.” Blocks $R_1$ and $R_2$ will synchronize to or desynchronize from $S_1$ depending on whether the incoming bit is “1” or “0.” By monitoring the error signals $e_1, e_2$ of $R_1, R_2$, one can then easily detect which bit has been transmitted, since the error signal of the synchronized system will drop almost to zero, while the other will be chaotic.

By a proper choice of $K_0, K_1$, the two chaotic waveforms can be safely distinguished at the receiver in spite of unavoidable tolerances on parameters (from Fig. 4(b), matching should be within 1%, typically). On the other side, it would be virtually impossible for the eavesdropper to decode the signal. Since the two chaotic orbits are close together, decoding cannot be performed by direct observation of the transmitted signal. Even if the system topology is known, and the receiver...
and the associated transmitted bit sequence. In this case, the synchronization error for bit 0 (the signal) at receiver 0.1 is the synchronization error for bit 0 (the signal) at receiver 0.1 for (not synchronized) and 20 Mb/s. We then recovered the digital 10 phase error 0.005. However, increasing the propagation delay, exceeding 0.1 for 50°. In practice, it is required to limit the maximum length of C within a few centimeters for efficient synchronization.

Finally, since fiber nonlinearity and dispersion could significantly distort the transmitted waveform and thus disturb synchronization, we have simulated the propagation of the modulated chaotic carrier through a fiber link. Though such effects should not be strong for a 1-mW 10-GHz signal, such investigation is worth doing because of the well-known sensitivity of chaos to perturbations. For nominal values of parameters (and neglecting attenuation, which has been considered above), we found that the error, after a 50-km dispersion-shifted fiber trunk, was not greater than \( \sigma_s = 0.005 \). As explained later, such a result could further be improved by filtering.

A possible electronic processing scheme to recover the transmitted bit sequence is as follows: first, the optical error signals from \( R_1 \) and \( R_2 \) are photodetected to get the envelopes \( S_{out,1}, S_{out,2} \); after filtering out the dc components, envelope detection followed by low-pass filtering is performed to get signals proportional to the chaos amplitude. Finally, subtracting the outputs from one another provides the reconstructed bits.

Neglecting the receiver noise and considering only the fluctuations due to synchronization error, it is easy to evaluate the signal-to-noise ratio. Following the outlined electronic processing, we can find for bit “0”

\[
S/N|_0 = \frac{\sigma_{s\infty}}{\sigma_{s10}} \tag{5}
\]

where \( \sigma_{s\infty} \) is the synchronization error for bit 0 (the signal) at receiver \( R_2 \) (not synchronized) and \( \sigma_{s10} \) is the synchronization error for bit 0 (the noise) at receiver \( R_1 \) (synchronized). In deriving (5), we have neglected the small dc component of \( E_1 - E_2 \) in (4) and we have assumed that the average is made on a time short with respect to the bit duration. A similar result applies to bit 1.

We have simulated the transmission of long random bit sequences, finding the SNR well in excess of 40 dB with the above parameter values. Since most noise is due to imperfect synchronization and is located around the relaxation frequency, this figure can be easily improved to more than 45 dB by filtering.

Better results could also be obtained by selecting wider spaced values for \( K \). However, working on too different orbits would finally enable an eavesdropper to understand the signal because the chaotic waveforms for the two digits become much different.

We have also simulated the transmission of a digital signal using the direct-injection scheme [5], to make a comparison. The chaotic carrier was modulated by a bit string, of amplitude \( 0.1 I_0 \) and bit rate \( f = 20 \text{ Mb/s} \). We then recovered the digital signal by subtracting the chaotic carrier obtained at the receiver

\[0.15\]
\[0.1\]
\[0.05\]
\[0.0\]
\[-0.05\]
\[-0.1\]

Fig. 8. Signal before CSK coding (square wave) and error signal from block \( R_1 \) after photodetection and high-pass filtering (\( S_{out,1} \)).
after synchronization to the transmitted signal, following the scheme proposed by the authors. The resulting SNR was less than 10 dB, but this figure could be almost doubled by filtering out high-frequency noise. However, we found it difficult to get further improvements since, by increasing the modulation depth, the bits became visible by direct inspection of the transmitted signal in the time domain. We believe that this reduced performance is due in part to the cryptographic scheme, which is not true CSK but rather amplitude modulation of a chaotic carrier (detected at the receiver as in masking cryptography [4]), in part to the lower performance of the synchronization method.

In conclusion, we have proposed a scheme to get effective and robust synchronization of backreflection chaotic lasers. Our proposal presents, together with greater simplicity with respect to that previously reported in [4], good performances of robustness and SNR and is suitable for CSK implementation.

REFERENCES


Valerio Annovazzi-Lodi (M’89) was born in Novara, Italy, on November 7, 1955. He received the degree in electronic engineering from the University of Pavia, Pavia, Italy, in 1979.

Since then, he has been working at the Department of Electronics of the University of Pavia in the field of electrooptics, formerly on injection modulation phenomena in lasers and on the fiber gyroscope, and later on birefringence effects in optical fibers, fiber sensors, and transmission via diffused infrared radiation. In 1983, he became a Staff Researcher of the Department of Electronics of the University of Pavia and in 1992 he became an Associate Professor at the same institution. He is the author of more than fifty papers and holds three patents.

Dr. Annovazzi-Lodi is a member of AEI.

Silvano Donati (M’75) graduated with a degree in physics from the University of Milan, Milan, Italy, in 1966.

For nine years, he was with CISE, Milan, working on noise in photomultipliers and avalanche photodiodes, nuclear electronics and electrooptic instrumentation (laser telemetry, speckle pattern interferometry, gated vision in scattering media). In 1975, he joined the Department of Electronics, University of Pavia, as an Internal Lecturer and worked on feedback interferometers, fiber gyroscopes, and noise in CCD’s. In 1980, he became full Professor of Optoelectronics, and since then his main research interests have been optical fiber sensors, passive fiber components for telecommunications, free-space and guided optical interconnections, and locking and chaos in lasers. He has authored or coauthored about 100 papers and holds four patents. He also worked in the standardization activity of CEI/EIC (CT-76 laser safety and CT-86 optical fibers).

Dr. Donati is a member of AEI, APS, OSA, and ISHM. He has participated in steering and program committees as a member or as a chairman.

Alessandro Scirè was born in Rimini, Italy, on June 26, 1971. He received the degree in electronic engineering cum laude from the University of Pavia, Pavia, Italy, in 1995. He is currently pursuing the Ph.D. degree in electronics and computer science at the same university.

Upon graduation, he worked for some months at the Electrooptics Laboratory of the University of Pavia before beginning his doctoral studies. His research interests are semiconductor lasers, injection phenomena, and chaos.