Secure communication scheme using chaotic laser diodes subject to incoherent optical feedback and incoherent optical injection

F. Rogister, A. Locquet, D. Pieroux, M. Sciamanna, O. Deparis, P. Mégret, M. Blondel

HAL Id: hal-03079991
https://hal.archives-ouvertes.fr/hal-03079991

Submitted on 17 Dec 2020

Secure communication scheme using chaotic laser diodes subject to incoherent optical feedback and incoherent optical injection

F. Rogister, A. Locquet

Advanced Research in Optics, Service d'Electromagnétisme et de Télécommunications,

Faculté Polytechnique de Mons, 31 Boulevard Dolez, B-7000 Mons, Belgium

D. Pieroux

Optique Nonlinéaire Théorique, Université Libre de Bruxelles, Campus Plaine C.P. 231,

B-1050 Bruxelles, Belgium

M. Sciamanna, O. Deparis, P. Mégret, M. Blondel

Advanced Research in Optics, Service d'Electromagnétisme et de Télécommunications,

Faculté Polytechnique de Mons, 31 Boulevard Dolez, B-7000 Mons, Belgium

We propose a secure communication scheme based on anticipating synchronization of two chaotic laser diodes respectively subjected to incoherent optical feedback and incoherent optical injection. This scheme does not require fine tuning of the optical frequencies of both lasers as it does for other schemes based on chaotic laser diodes subject to coherent optical feedback and injection. Our secure communication scheme is therefore attractive for experimental investigation.

Synchronization of chaotic oscillators and its application to secure communications has attracted considerable interest during the last decade [1-4]. In particular, laser diodes subject to delayed, coherent optical feedback revealed themselves good candidates for secure communications. Indeed their large bandwidth and their high dimensional chaotic dynamics lead to a high security level [5,6]. However, in such schemes implementing single-mode laser diodes subject to coherent optical feedback, the synchronization performance depends on the detuning between the free-running frequencies of the transmitter and the receiver lasers. In particular, a few hundred MHz negative detuning of the receiver frequency relative to the transmitter one leads to a large degradation of the synchronization [7]. From a practical point of view, it is therefore interesting to investigate alternative cryptographic schemes that would not require fine tuning of the optical frequencies.

In this Letter, we propose a novel secure communication scheme based on anticipating synchronization [8] of two chaotic laser diodes in which the transmitter laser is subject to incoherent optical feedback and the receiver laser is coupled to the transmitter laser via incoherent optical injection. The message is encrypted by chaos shift keying [9]. In this scheme, the feedback and injected fields act on the population inversion in the laser active layers but do not interact coherently with the intracavity lasing fields. As a consequence, the phases of the feedback and injection fields do not intervene on the lasers dynamics. For that reason, the secure communication scheme we propose does not require fine tuning of the optical frequencies of both lasers. This scheme is therefore attractive for experimental realization.

In the scheme we propose (Fig. 1), the linearly polarized output field of the transmitter laser first undergoes a 90° polarization rotation through an external cavity formed by a Faraday

rotator (FR) and a mirror. It is then splitted in two parts by a non-polarizing beam splitter (BS): one part is fed back into the transmitter laser and the other part is injected into the receiver laser. Polarization directions of feedback and injection fields are orthogonal to those of transmitter and receiver output fields, respectively. In other words, the transmitter laser is subject to incoherent feedback while the receiver one is subject to incoherent injection. An optical isolator (ISO) shields the transmitter from parasitic reflections from the receiver. Tunable attenuators (not shown in Fig. 1) adjust the respective strengths of the feedback and the injection. If necessary, a linear polarizer (LP) may be placed between the Faraday rotator and the mirror to prevent coherent feedback induced by a second round-trip in the external cavity after reflection on the transmitter laser front facet. In order to encode a message, the current of the transmitter laser is switched between two discrete values corresponding respectively to bits "0" and "1".

The model used to describe the dynamics of the system is an extension of the model proposed by Otsuka and Chern for semiconductor lasers subject to incoherent optical feedback [10]:

$$\frac{dP_1}{dt} = \left(G_1 - \frac{1}{\tau_{p1}} \right) P_1(t) + \beta_1 N_1(t) + F_1(t) , \qquad (1)$$

$$\frac{dN_1}{dt} = \frac{I_1(t)}{e} - \frac{N_1(t)}{\tau_{s1}} - G_1 \left[P_1(t) + \kappa P_1(t - \tau) \right], \qquad (2)$$

and

$$\frac{dP_2}{dt} = \left(G_2 - \frac{1}{\tau_{p2}} \right) P_2(t) + \beta_2 N_2(t) + F_2(t) , \qquad (3)$$

$$\frac{dN_2}{dt} = \frac{I_2}{e} - \frac{N_2(t)}{\tau_{s2}} - G_2 \left[P_2(t) + \sigma P_1(t - \tau_c) \right] \qquad (4)$$

where $G_j = G_{Nj} \left[1 - \varepsilon_j P_j \right] \left[N_j - N_{0j} \right]$ with $j = 1$ for the transmitter and $j = 2$ for the receiver. In these equations, P_j and N_j are the photon number and the electron-hole pair number in the active region of laser j. N_{0j} is the value of N_j at transparency. τ_{pj}, τ_{sj}, I_j, G_{Nj} and ε_j are respectively the photon lifetime, the carrier lifetime, the injection current, the gain coefficient and the gain saturation coefficient of laser j. e is the electronic charge. F_j is a Langevin noise force that accounts for stochastic fluctuations arising from spontaneous emission process. The Langevin forces satisfy the relations $< F_j(t) F_j(t') > = 2 N_j P_j \beta_j \delta(t - t')$, where β_j is the spontaneous emission rate. The operating parameters κ, τ and σ are respectively the strength and the delay of the feedback at the transmitter, and the coupling strength at the receiver. The duration taken by the light emitted by the transmitter to reach the receiver is τ_c. We use typical values for the internal parameters of the transmitter laser: $\tau_{p1} = 2$ ps, $\tau_{s1} = 2$ ns, $G_{N1} = 1 \times 10^4$ s^{-1}, $N_{01} = 1.1 \times 10^8$, $\beta_1 = 5 \times 10^3$ s^{-1} and $\varepsilon_1 = 7.5 \times 10^{-8}$. In a first step, the parameters at the receiver are chosen identical to those of the transmitter. Afterwards, we will consider slight differences between the corresponding parameters.

In absence of the stochastic terms F_j and for identical internal and operating parameters, the exact synchronous solution,

$$P_2(t) = P_1(t - \Delta t), \ N_2(t) = N_1(t - \Delta t), \quad (5)$$

where $\Delta t = \tau_c - \tau$ is the synchronization lag, exists only if the injection strength at the receiver matches exactly the feedback strength at the transmitter, i.e. $\sigma = \kappa$. It should be noted that this condition is not sufficient to observe synchronization between the two lasers since the solution (5) can be stable or unstable. Eq. (5) means that the state of the receiver at time t can synchronize to the state of the transmitter at time $t - \tau_c + \tau$. In other words, the receiver anticipates the signal that will be injected at time $t + \tau$. The anticipation time is τ, the feedback delay at the transmitter. Anticipating synchronization has been demonstrated recently to result from the interaction between delayed feedback and dissipation and to be a rather universal phenomenon in nonlinear dynamical systems with unidirectional coupling [8]. It has also been predicted in coupled laser diodes subject to delayed coherent optical feedback [7,11].

The synchronization between the two lasers is robust with respect to stochastic fluctuations induced by spontaneous emission as shown in Fig. 2. The feedback strength and delay at the transmitter are $\kappa = 0.41$ and $\tau = 9$ ns respectively. The coupling strength matches exactly the feedback strength at the transmitter, i.e. $\sigma = \kappa$. Injection currents of the two lasers are $I_j = 1.8 \times I_{thj}$, j= 1,2, where I_{thj} is the threshold current of laser j. For these values, the output of the transmitter laser is chaotic [Fig. 2(a)]. At time t, the receiver output synchronizes almost perfectly to the transmitter output at time $t - \Delta t$ [Fig. 2(b)]. The good quality of the synchronization is shown on the synchronization diagram where the output of the receiver at time t is plotted versus the output of the transmitter at time $t - \Delta t$ [Fig. 2(c)]. Since in case of perfect synchronization, the points would lie on a straight line [Eq. (6)], the synchronization

quality can be characterized by computing the linear correlation coefficient r. For the values of parameters we use, r = 0.993 indicating a good level of synchronization. The synchronization is also robust to small mismatches between corresponding parameters in both systems. The correlation coefficient remains above 0.9 if discrepancies between the transmitter and the receiver parameters are within 1% difference. It is worthwhile to note that a 1% mismatch between the gain coefficients corresponds to a frequency detuning of several hundreds of GHz if the frequency dependence of the gain is taken into account [12].

The message encoding is achieved by chaos shift keying [9]. The bit stream modulates the injection current at the transmitter, i.e. bits "0" and "1" correspond to two different values of the injection current. Here we choose to use $\iota_0 = 1.8 \times I_{th,1}$ and $\iota_1 = 1.003 \times \iota_0$ respectively. At the receiver, a replica of the transmitter laser is used. The injection current at the receiver I_2 is set to ι_0. Message decoding is achieved by computing the normalized synchronization error

$\Delta P = (P_1(t - \Delta t) - P_2(t)) / P_0$ where P_0 is the mean value of the receiver output in absence of optical injection. The synchronization error is low-pass filtered by a four-order Butterworth filter with a cut-off frequency of 1.3 B, where B is the bit rate. Bits "0" are then detected when the filtered synchronization error is close to zero. By contrast, bits "1" are detected when the synchronization error is large due to the mismatch between the injection currents. Fig. 3 shows a 250 Mbit/s message transmission for lasers chosen identical and with stochastic terms $F_{1,2}(t)$ taken into account. We have checked that the encoded bits cannot be detected by direct observation in the time domain or after filtering the transmitted signal [13]. The robustness of the synchronization to small mismatches (typically of the order of 1%) between homologous internal and operating parameters makes the cryptographic scheme we proposed practically

feasible. However, the sensitivity of the synchronization on larger mismatches of parameters, especially the injection current, the carrier and the photon lifetimes, allows a high level of security since the replication of the system by eavesdropper is difficult. Finally, as for other secure communication schemes using delayed feedback, the high dimension of the chaos induced by the delay term complicates eavesdropping through reconstruction of the embedding phase space.

In conclusion, we propose a novel secure communication scheme based on anticipating synchronization of laser diodes subject to incoherent optical feedback and injection. This scheme is remarkable in that it requires no fine tuning of the laser optical frequencies, contrary to other schemes based on laser diodes subject to coherent optical feedback. This is due to the absence of interaction between, on the one hand, the intracavity fields and, on the other hand, the injected and fed back fields, these later interacting only with the carrier density. Our secure communication scheme is therefore attractive for experimental and operational investigations.
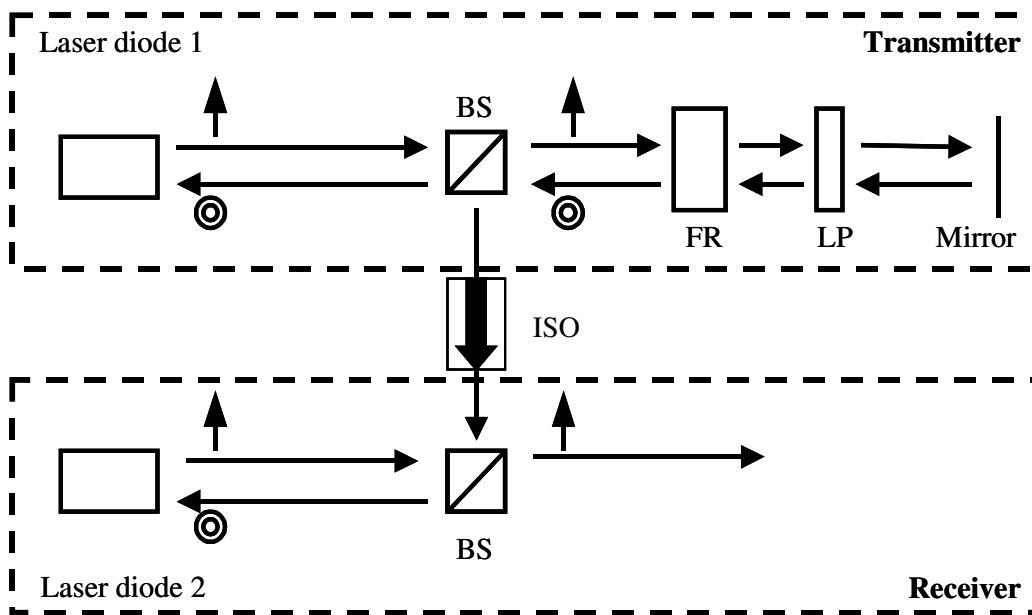
References

1. L.M. Pecora and T.L. Carrol, Phys. Rev. Lett. **64**, 821 (1990).

2. K.M. Cuomo and A.V. Oppenheim, Phys. Rev. Lett. **71**, 65 (1993).

3. J.P. Goedgebuer, L. Larger, and H. Porte, Phys. Rev. Lett. **80**, 2249 (1998).

4. G.D. Van Wiggeren and R. Roy, Science **279**, 1198 (1998).

5. C.R. Mirasso, P. Colet, and P. García-Fernández, IEEE Photonics Technol. Lett. **8**, 299 (1996).

6. V. Annovazzi-Lodi, S. Donati, and A. Scire, IEEE J. Quantum Electron. **33**, 1449 (1997).

7. Y. Liu, H.F. Chen, J.M. Liu, P. Davis, and T. Aida, Phys. Rev. A **63**, 031802(R) (2001).

8. H.U. Voss, Phys. Rev. E **61**,5115 (2000).

9. H. Dedieu, M.P. Kennedy, and M. Hasler, IEEE Trans. Circuits Syst. II **40**, 634 (1993).

10. K. Otsuka and J-L. Chern, Opt. Lett. **16**, 1759 (1991).

11. V. Ahlers, U. Parlitz, and W. Lauterborn, Phys. Rev. E **58**, 7208 (1998); C. Masoller, Phys. Rev. Lett. **86**, 2782 (2001).

12. G.P. Agrawal and N.K. Dutta, Long-wavelength semiconductor lasers, (Van Nostrand Reinhold, New York, 1986).

13. Butterworth and Chebyshev filters have been used to recover the message without success.
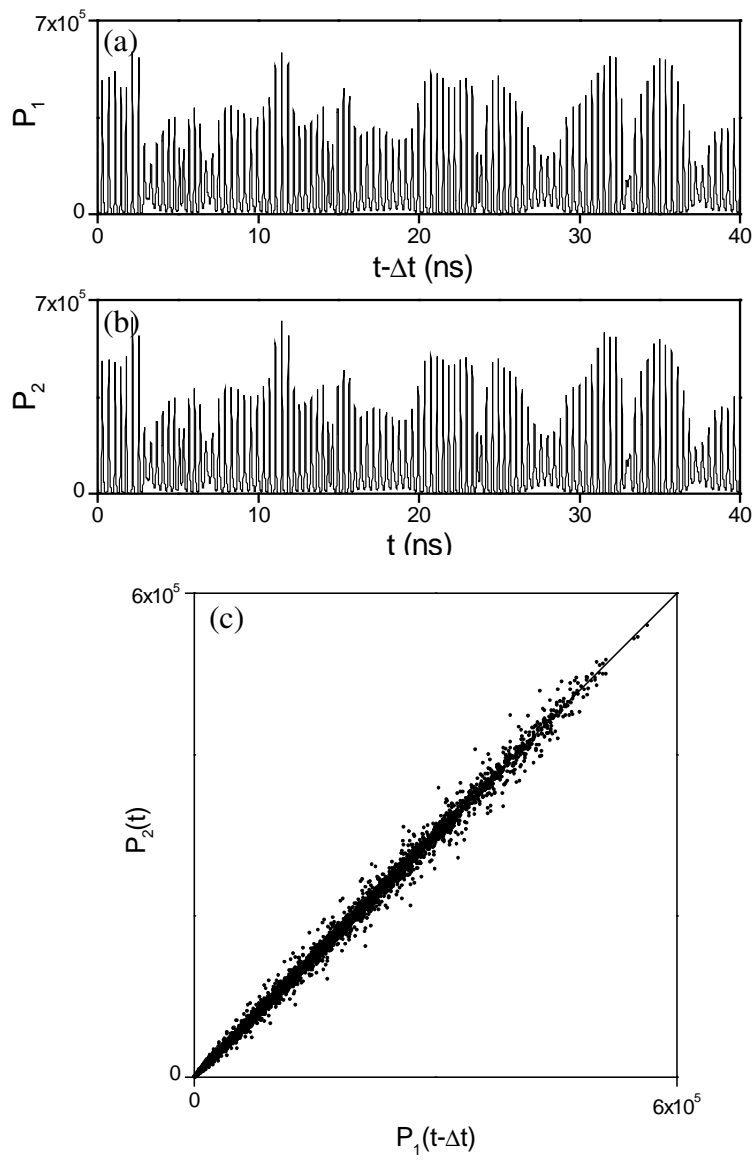
Figure captions

Fig. 1. Schematic representation of the secure communication scheme. See text for definitions.

Fig. 2. (a) Output of the transmitter shifted by Δt. (b) Output of the receiver laser. (c) Synchronization diagram of the receiver output $P_2(t)$ versus the transmitter output $P_1(t-\Delta t)$. The laser parameters are identical and the injection current at the transmitter is not modulated. The stochastic terms $F_{1,2}(t)$ are taken into account.
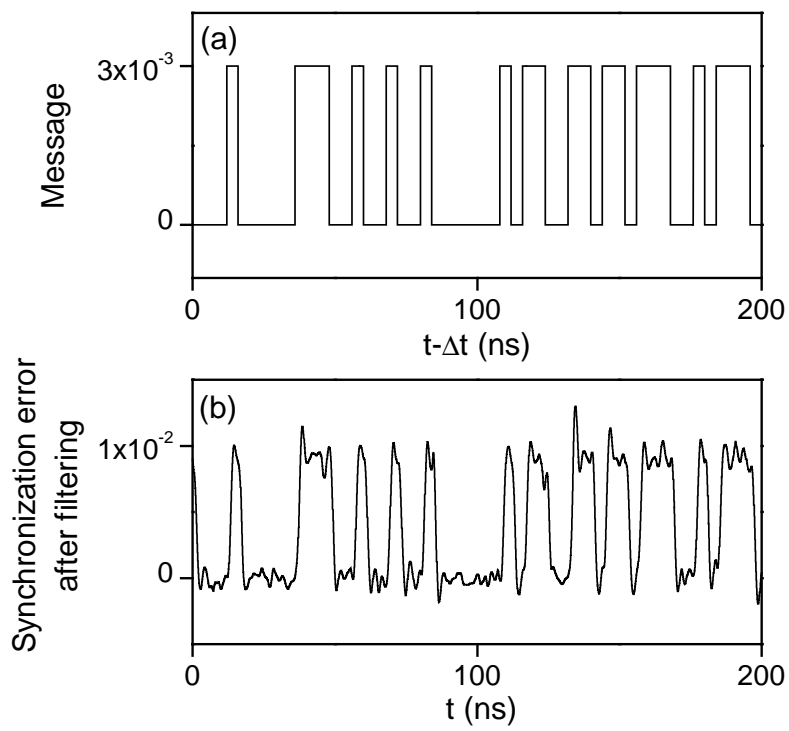
Fig. 3. (a) Encoded message at a bit rate of 250 Mbit/s. (b) Synchronization error after filtering.

Rogister et al., Fig. 1

Rogister et al., Fig. 2

(a)

3×10^{-3}

Message

0

0   100   200

t-Δt (ns)

(b)

1×10^{-2}

Synchronization error
after filtering

0

0   100   200

t (ns)

Rogister et al., Fig. 3