Proceedings Symposium IEEE/LEOS Benelux Chapter, 2000, Delft, The Netherlands

New cryptographic scheme using semiconductor laser diodes subject to external optical feedback

A. Locquet, F. Rogister, P. Mégret and M. Blondel[1]
Advanced Research in Optics, Service d'Electromagnétisme et de Télécommunications,
Faculté Polytechnique de Mons, 31 Boulevard Dolez, B-7000 Mons, Belgium
Tel : + 32 (65) 374198 ; Fax : + 32 (65) 374199 ; E-mail : Locquet@telecom.fpms.ac.be

A cryptographic scheme using two synchronized chaotic semiconductor lasers subject to external optical feedback is investigated numerically. Unlike the schemes that have been proposed so far, the information signal is not just mixed with the chaotic signal produced by the transmitter laser but it is also injected into the dynamics of this external-cavity laser. This makes it more difficult to unmask the cryptographic scheme. Depending on the values of some parameters of the transmitter and receiver lasers, we observe either a "classic" synchronization or a novel type of synchronization, called anticipating synchronization, in which the receiver synchronizes with a future state of the transmitter.

I Introduction

Secure communication using chaotic signals has attracted much attention since the discovery of synchronized chaos [1]. We will present in this paper a new cryptographic scheme that is based on the "chaotic masking" technique. In this kind of technique, the message is added to a chaotic "carrier" produced by the transmitter system. The transmitted signal is injected into the receiver system, which synchronizes, after a transient, with the chaotic carrier produced by the transmitter. The message is extracted at the receiver by subtracting the chaotic carrier reproduced at the receiver from the transmitted signal.
Chen and Liu [2] have devised a scheme that uses semiconductor lasers subject to external injection and in which the message is not just added to the output of the transmitter laser but is also injected into its dynamics. Therefore the chaotic carrier itself is dependent on the message and it will be more difficult for an eavesdropper to extract the message by predicting locally the dynamics of the chaotic carrier [3] precisely because this carrier is also a function of the unknown message.
In this paper, we propose two new cryptographic schemes in which the message is injected into the dynamics of the transmitter and is added to the output of this transmitter but contrary to [2], external-cavity lasers are used. The advantage of this scheme over [2] relies on the fact that the delay introduced by the external cavity creates an infinite dimensional phase space and therefore the chaotic signals produced by external-cavity lasers *can* be very hyperchaotic (i.e. can possess a very large number of positive Lyapounov exponents). The use of hyperchaotic signals has precisely been proposed as a way of increasing the security level of chaotic optical cryptography [4].

In section II, we present the two new cryptographic schemes. The first one is based on synchronization in the usual sense and the second one is based on a novel type of synchronization called anticipating synchronization [5].

[1] This work is supported by the "Fond Halleux-Mirland" of the AIMS. P.M. and F.R. are supported by the Inter-University Attraction Pole program (IAP IV/07) of the Belgian governement (SSTC).

II Cryptographic schemes proposed

II.1 Scheme using « Classic » synchronization

Figure 1 represents the first cryptographic scheme proposed. The transmitter and the receiver are two identical single-mode external-cavity lasers. The message is a binary pseudo-random bipolar signal whose complex electric field is $m(t)\cdot e^{i\cdot\omega_{0,m}\cdot t}$. This signal is injected into the laser cavity through its left facet and is also added to the laser output. At the receiver, the transmitted signal is injected into the laser cavity through its left facet. The coupling attenuators (CA) and the neutral density filters (NDF) are used to control the power injected and reflected back into the laser cavities.

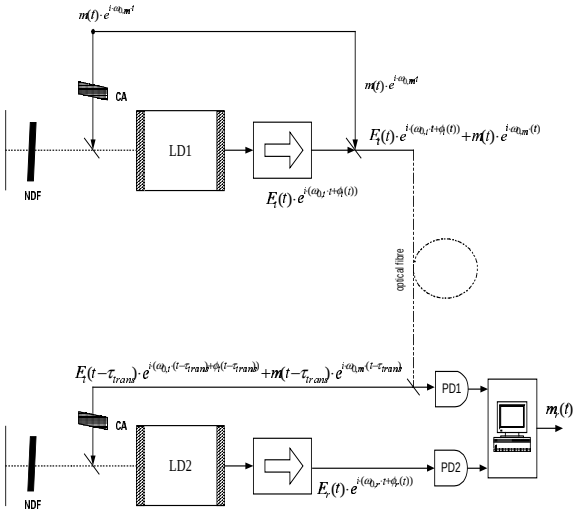

FIG. 1. Cryptographic scheme using « classic » synchronization

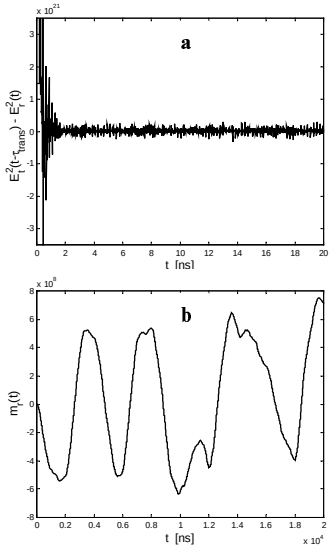

FIG. 2. Synchronization error (a) and reconstructed signal (b).

The model used is based on the Lang and Kobayashi equations [6]. It can be easily found that the equations for the carrier density and the complex amplitude of the electric field for the transmitter (t) and the receiver (r) are :

$$\frac{d(E_t(t)\cdot e^{i\cdot\phi_t(t)})}{dt}=\left\{\frac{1}{2}\cdot[1+i\cdot\alpha]\cdot\left[G_t(t)-\frac{1}{\tau_p}\right]\right\}\cdot E_t(t)\cdot e^{i\cdot\phi_t(t)}$$
$$+\gamma_t\cdot E_t(t-\tau)\cdot e^{i\cdot\phi_t(t-\tau)}\cdot e^{-i\cdot\omega_{0,t}\cdot\tau}+\gamma_{ext,1}\cdot m(t)\cdot e^{i\cdot(\omega_{0,m}-\omega_{0,t})\cdot t} \quad (1)$$

$$\frac{dN_t(t)}{dt}=J-\frac{N_t(t)}{\tau_S}-G_t(t)\cdot E_t{}^2(t) \quad (2)$$

$$\frac{d(E_r(t)\cdot e^{i\cdot\phi_r(t)})}{dt}=\left\{\frac{1}{2}\cdot[1+i\cdot\alpha]\cdot\left[G_r(t)-\frac{1}{\tau_p}\right]\right\}\cdot E_r(t)\cdot e^{i\cdot\phi_r(t)} \quad (3)$$
$$+\gamma_r\cdot E_r(t-\tau)\cdot e^{i\cdot\phi_r(t-\tau)}\cdot e^{-i\cdot\omega_{0,r}\cdot\tau}+\gamma_{ext,2}\cdot E_t(t-\tau_{trans})\cdot e^{i\cdot\phi_t(t-\tau_{trans})}\cdot e^{i\cdot(\omega_{0,t}-\omega_{0,r})\cdot t}\cdot e^{-i\cdot\omega_{0,t}\cdot\tau_{trans}}$$
$$+\gamma_{ext,2}\cdot m(t-\tau_{trans})\cdot e^{i\cdot(\omega_{0,m}-\omega_{0,r})\cdot t}\cdot e^{-i\cdot\omega_{0,m}\cdot\tau_{trans}}$$

$$\frac{dN_r(t)}{dt}=J-\frac{N_r(t)}{\tau_S}-G_r(t)\cdot E_r{}^2(t) \quad (4)$$

In the preceding equations, the different parameters have the same meaning and the same values as in [7] and in addition τ_{trans} is the propagation time of light between the transmitter and the receiver, $\omega_{0,t} = \omega_{0,r} = \omega_{0,m} = \omega_0$ are the angular frequencies of the solitary transmitter and receiver lasers and the angular frequency of the laser used to produce the message respectively, $\gamma_t = \gamma_r = 2 \cdot 10^{10}\, s^{-1}$, $\gamma_{ext,1} = \gamma_{ext,2} = 5 \cdot 10^{10}\, s^{-1}$ where γ_t, γ_r are the feedback coefficients of the transmitter and receiver lasers respectively and $\gamma_{ext,1}$, $\gamma_{ext,2}$ the injection coefficients in the transmitter and receiver lasers respectively.

Photodiode PD1 produces an output proportional to the power injected into the receiver, $\left|E_t(t) \cdot e^{i \cdot \phi_t(t)} + m(t)\right|^2 = E_t^2(t) + m^2(t) + 2 \cdot E_t(t) \cdot m(t) \cdot \cos(\phi_t(t))$; the output of PD2 is proportional to the output power of the receiver $E_r^2(t) \approx E_t^2(t)$. The synchronization error on the power of the electric field is represented in figure 2. After a short transient, this error becomes bounded and small. Figure 2 shows also the message reconstructed at the receiver by subtracting the outputs of the two photodiodes and by low-pass filtering the difference signal in order to eliminate the interference term $2 \cdot E_t(t) \cdot m(t) \cdot \cos(\phi_t(t))$. Like in any chaotic masking scheme, for efficient suppression of the interference term the message has to be transmitted at a lower frequency than the typical frequency (several GHz) of the chaotic carrier fluctuations. We have used in these simulations a bit rate of 0.25 Mbit/s.

II.2 Scheme using anticipating synchronization

The cryptographic scheme proposed is represented in figure 3. This time, the message that is injected into the transmitter laser, $m(t) \cdot e^{i \cdot \omega_{0,m} \cdot t}$, is a delayed version (with a delay equal to τ) of the message $m(t+\tau) \cdot e^{i \cdot \omega_{0,m} \cdot (t+\tau)}$ that is added to the chaotic carrier.

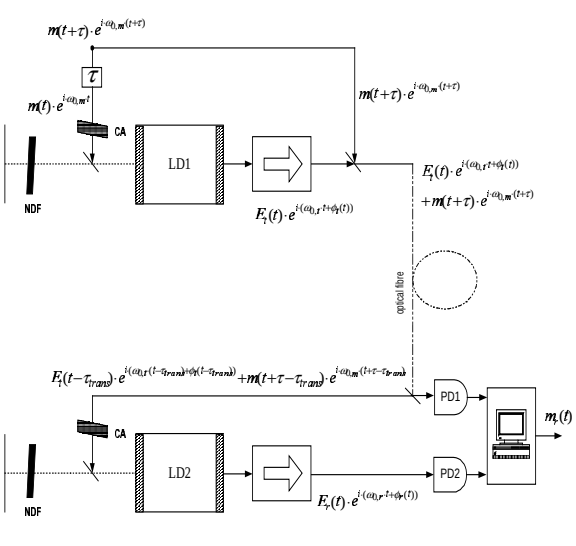

FIG. 3. Cryptographic scheme using anticipating synchronization

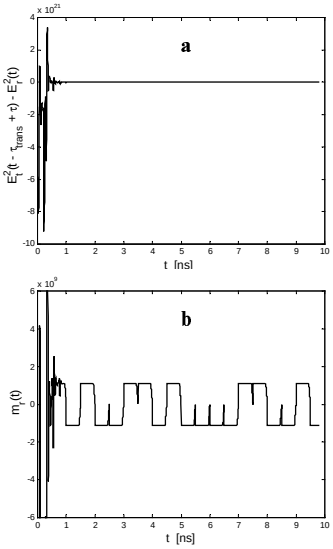

FIG. 4. Synchronization error (a) and reconstructed signal (b).

The equations of this scheme are given in [8] and it has been found that a synchronized solution $\{E_r(t) = E_t(t-\tau_{trans}+\tau), \phi_r(t) = \phi_t(t-\tau_{trans}+\tau) - \omega_0 \cdot (\tau_{trans}-\tau), N_r(t) = N_t(t-\tau_{trans}+\tau)\}$ exists if all the homologous parameters of the receiver and of the transmitter are equal and if $\eta_t = \eta_r + \eta_{ext,2}$ and $\eta_{ext,1} = \eta_{ext,2}$. This means that at time t, the receiver produces an output that is equal to the chaotic carrier that will be injected into it at time $t+\tau$. Therefore the receiver laser anticipates the dynamics of the transmitter laser.
Figure 4 represents the synchronization error. After a short transient, this error becomes equal to zero, confirming the fact that perfect synchronization occurs[2]. Since the synchronization is perfect, the interference term is null and therefore the bit rates that can be transmitted are higher than with the first scheme, if the transmitter and receiver lasers are identical. A message at 1Gbit/s has been transmitted and the reconstructed signal is represented in figure 4. The reconstruction is perfect and no filtering is needed in this case.
An important issue is the robustness of these two cryptographic schemes to mismatches between homologous parameters of the transmitter and the receiver. Numerical simulations show that, for both schemes, the quality of the *synchronization* is not significantly affected if the mismatches are limited to a few percent. However the presence of an interference term in the second scheme induces a reduction of the bit rate of the message.

III Conclusion

We have proposed two new cryptographic schemes that possess a higher security level than the conventional chaotic masking schemes because the message is not just added to the chaotic carrier but is also injected into the dynamics of the transmitter laser. Moreover, the use of chaos generated by an external cavity laser means that very hyperchaotic carriers can be generated, which is also believed to increase the secrecy of the transmission. However, the real security level of this scheme, and of the other schemes using chaotic optical cryptography, is an issue that has still to be clarified.

IV References

[1] L.M.Pecora and T.Carroll, " Synchronization in chaotic systems ", *Phys .Rev. Lett.,* **64**, 19 February 1990, pp.821-824.
[2] H.F.Chen and J.MLiu, "Open-loop chaotic synchronization of injection-locked semiconductor lasers with gigahertz range modulation", *IEEE J.Quantum Electron.,* **36**, January 2000, pp.27-34.
[3] K.M.Short, " Steps towards unmasking secure communications ", *Int. J.Bifurcation and Chaos*, **4**, No.4, 1992, pp.959-977.
[4] J.-P. Goedgebuer, L.Larger, and H.Porte, " Optical cryptosystem based on synchronization of hyperchaos generated by a delayed feedback tunable laser diode ", *Phys.Rev.Lett.,* **80**, 9 March 1998, pp.2249-2259.
[5] H.U.Voss, " Anticipating chaotic synchronization ", *Phys .Rev. E.,* **61**, May 2000, pp.5115-5119.
[6] R.Lang and K.Kobayashi, " External optical feedback effects on semiconductor injection laser properties ", *IEEE J.Quantum Electron.,* 16, March 1980, pp.347-355.
[7] A.Sanchez-Diaz, C.Mirasso, P.Colet and P.Garcia-Fernandez, " Encoded Gbit/s Digital communication with synchronized chaotic semiconductor lasers ", *IEEE J.Quantum Electron.,* **35**, 3 March 1999, pp.292-297.
[8] A.Locquet, " Etude de la cryptographie basée sur le comportement chaotique des lasers à semi-conducteurs ", Final year thesis, *Faculté Polytechnique de Mons,* July 2000.

[2] We put emphasis on the fact that we have supposed that homologous parameters of the transmitter and receiver are equal.