Public-channel cryptography based on mutual chaos pass filters

Einat Klein,[1] Noam Gross,[1] Evi Kopelowitz,[1] Michael Rosenbluh,[1] Lev Khaykovich,[1] Wolfgang Kinzel,[2] and Ido Kanter[1]
[1]*Department of Physics, Bar-Ilan University, Ramat-Gan, 52900 Israel*
[2]*Institut für Theoretische Physik, Universität Würzburg, Am Hubland 97074 Würzburg, Germany*
(Received 28 February 2006; published 2 October 2006)

We study the mutual coupling of chaotic lasers and observe both experimentally and in numeric simulations that there exists a regime of parameters for which two mutually coupled chaotic lasers establish isochronal synchronization, while a third laser coupled unidirectionally to one of the pair does not synchronize. We then propose a cryptographic scheme, based on the advantage of mutual coupling over unidirectional coupling, where all the parameters of the system are public knowledge. We numerically demonstrate that in such a scheme the two communicating lasers can add a message signal (compressed binary message) to the transmitted coupling signal and recover the message in both directions with high fidelity by using a mutual chaos pass filter procedure. An attacker, however, fails to recover an errorless message even if he amplifies the coupling signal.

DOI: 10.1103/PhysRevE.74.046201 PACS number(s): 05.45.Vx, 42.55.Px, 42.65.Sf

Coupled semiconductor lasers have been studied extensively in recent years, due to their inherent nonlinearity and chaotic dynamics. Chaos synchronization for two unidirectionally coupled lasers, each of which also has self-feedback from an external cavity, has been demonstrated experimentally and theoretically in [1–3]. In addition, mutually coupled semiconductor lasers were also studied extensively [4–7] and revealed different and interesting dynamics. Chaos synchronization has attracted even more interest recently, because of its potential application in optical secret communication systems [8–10].

In this paper the synchronization properties of mutually coupled versus unidirectionally coupled lasers are analyzed and compared. We show that there exists a regime in the coupling parameter space for which the mutually coupled lasers synchronize very well, yet a unidirectionally coupled laser does not. Thus in an application in which synchronization is desirable, mutually coupled lasers have an advantage.

We use this result to propose a secret communication scheme over a public channel based on this advantage of mutual coupling over unidirectional coupling. We emphasize the public-channel nature of the proposed scheme and the advantages this brings to cryptographic communication systems that make use of chaos synchronization. For unidirectionally coupled lasers, chaos synchronization cryptography has been based on a private-key procedure, where the two communicating parties have a common secret key prior to the communication process, which they use to encrypt the message they wish to transmit. The unidirectionally coupled lasers are usually synchronized in a master-slave configuration, and the secret key generally consists of the system's parameters [8]. The system parameters provide a private key because the two communicating lasers must have identical (or nearly identical) parameters, or else synchronization is impossible. In this paper we propose an all-optical *public*-channel cryptographic system, in which there is no need to conceal any of the system's parameters or to exchange private information prior to the public-channel communication process.

In our proposed system, the two communicating lasers are mutually coupled in such a way that they exhibit isochronal synchronization, in which there is no delay in their synchronized signals. Stable isochronal synchronization is achieved due to the self-feedback of each laser as described in [12]. Message encryption is accomplished by adding a low-amplitude binary message to the chaotic laser fluctuations so that the ensuing transmitted signal still appears to be chaotic and random. Both lasers are allowed to send, simultaneously, independent messages to each other and the messages are independently recovered at both ends of the communication line, ensuring bidirectional information flow. At the receiving end, both lasers use a chaos pass filter procedure to decode the message from the received chaotic signal which we will call a "mutual chaos pass filter" (MCPF) procedure.

Communication security is based on the fact that a third laser, labeled the "attacker," who tries to synchronize himself to the transmitted signals, is disadvantaged compared to the mutually coupled lasers, and although he can manage to partly recover the message, he has considerably more error bits in his recovered message, and so his eavesdropping attack can be considered unsuccessful. The use of the MCPF procedure provides two novel and distinct advantages: it is public key—i.e., it does not require a secret key prior to communication—and it allows for simultaneous bidirectional communication.

Our experimental setup is schematically depicted in Fig. 1, where two mutually coupled external feedback lasers *A* and *B* represent the communicating pair and the third laser *C* which is identically configured but coupled unidirectionally to one of the pair represents the attacker. For reasons of convenience we chose to work in the LFF regime. In the experiments we use three single-mode lasers *A*, *B*, and *C*, emitting at 660 nm and operating close to their threshold. The temperature of each laser is stabilized to better than 0.01 K, and all are subjected to a similar optical feedback. The length of the external cavity is equal for all lasers and is set to 180 cm (round-trip time 12 ns). The feedback strength of each laser is adjusted using a $\lambda/4$-wave plate and a polarizing beam splitter. The two lasers (*A* and *B*) are mutually coupled by injecting a fraction of each one's output power to the other. Coupling powers are adjusted using a neutral-density filter. The attacker laser (*C*) is coupled unidirectionally to one of the mutually coupled lasers, with unidi-

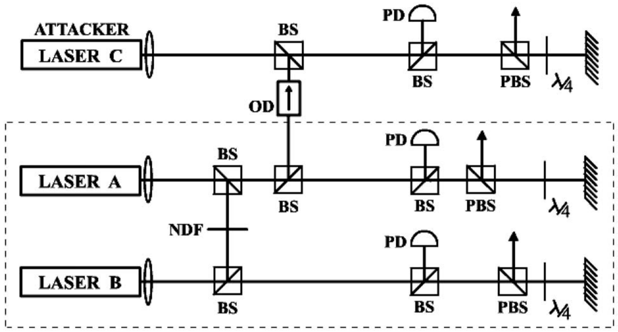

FIG. 1. Schematic diagram of the experimental setup. Lasers *A* and *B* are mutually coupled, and *C*, the attacker, is unidirectionally coupled. BS, beam splitters; PBS, polarization beam splitters; OD, optical isolator; PD, photodetectors.

rectionality ensured by an optical diode (−33 dB). All the coupling optical paths are set to be equal to the self-feedback round-trip path. Three fast photodetectors (response time <500 ps) are used to monitor the laser intensities which are simultaneously recorded with a digital oscilloscope (500 MHz, 1 GS/s) [14].

For the case of unidirectionally coupled lasers two types of synchronization, identical and generalized, have been observed [15,16]. In our experiments we have focused on the identical synchronization (which is isochronal); i.e., the two lasers receive the same total feedback intensities [17].

We compare mutual versus unidirectional coupling over a range of coupling and self-feedback strengths, denoted σ and κ, respectively. In the experiment the total feedback intensity is such that it results in the reduction of the solitary laser's threshold current by approximately 5%. While keeping the total feedback of all lasers equal [11], we vary the values of σ and κ over the entire parameter space. The degree of synchronization between the lasers is evaluated via the cross-correlation function [12]. The time-dependent intensity traces are divided into 10 ns segments (containing ten sample points), and the overlap between matching segments is calculated and arranged in a histogram. We find that for mutual coupling robust and stable synchronization is obtained at least from $\kappa=2\sigma$ to $\kappa=0.5\sigma$ (see also Ref. [12]). For the case of unidirectional coupling, good synchronization is found for $\kappa=0$ of the receiver, but it deteriorates quickly as we increase the part of κ in the total feedback of the receiver [16].

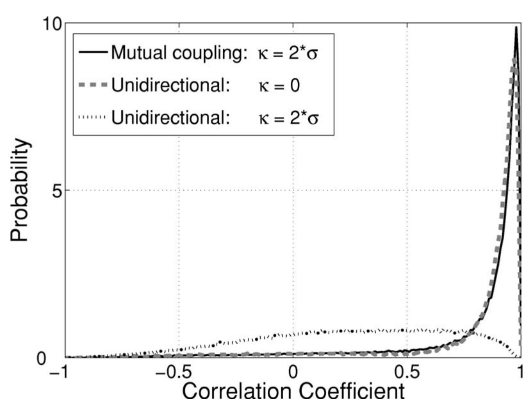

FIG. 2. Correlation coefficient histograms for intensity traces divided into 10-ns segments, for the cases of mutual and unidirectional coupling. The total feedback strength is equal in all cases.

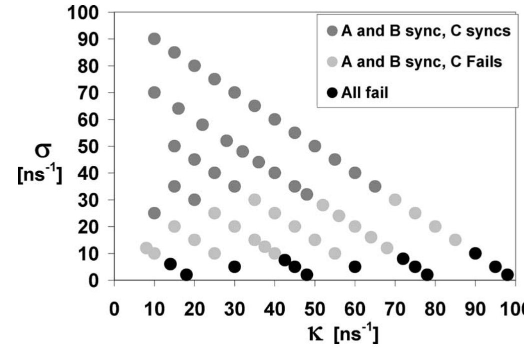

FIG. 3. Success or failure of synchronization for the parties and attacker for a range of parameter values: κ, feedback strength, and σ, coupling strength.

In Fig. 2 we show a representative point in the parameter phase space where mutual coupling is advantageous over unidirectional coupling by presenting a comparison of overlap histograms for three situations: mutual coupling $\kappa=2\sigma$, unidirectional coupling $\kappa=0$, and unidirectional coupling $\kappa=2\sigma$. While the first two show good synchronization with a mean value of 0.84, the third is significantly worse.

The advantage of mutual coupling over unidirectional is also obtained in our numerical simulations. We calculate the system behavior using the Lang-Kobayashi differential equations, as defined in [13] [and also in Eq. (1) below, when taking $M=0$]. For the dynamics parameters we used the values in [13] and the two lasers *A* and *B* were found to be synchronized isochronally [12,17].

We now discuss the two-dimensional phase space, defined by parameters κ and σ of lasers *A* and *B* and the attacker to either *A* or *B*. This phase space is characterized by the following three regimes as depicted in Fig. 3: the dark gray regime where σ is strong enough in comparison to κ and all lasers are synchronized and the black regime where the coupling is negligible and there is a lack of synchronization between any of the lasers. Most interesting is the window of the light gray regime where *A* and *B* are synchronized, but *C*

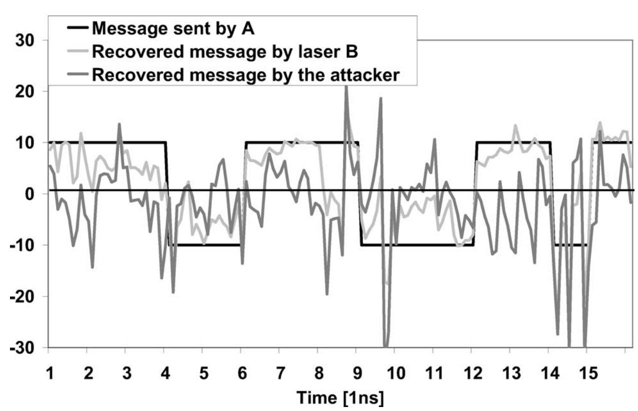

FIG. 4. A trace of the message sequence sent from laser *A* to *B* (black), which consists of 111001110001101, the recovered message by *B* (light gray), and the recovered message by the attacker (dark gray). The parameters used by *A* and *B* are $\kappa=110$ ns^{-1}, $\sigma=40$ ns^{-1}. The attacker amplifies the coupling signal to a maximum and uses $\kappa=0$, $\sigma=150$ ns^{-1}.

fails to synchronize (we define failure when the average correlation is less than 0.7). It is in this regime that mutual coupling is superior to unidirectional coupling; thus, even if laser C uses the exact same parameters as lasers A and B, the fact that he is not mutually coupled to A or B but only listening, affects his synchronization ability. This new effect has been observed in other chaotic systems as well [18] and is at the center of our proposed cryptographic system presented below. Note that if the attacker amplifies the coupling signal and uses a stronger σ (outside the light gray regime) such as $\sigma_{attacker}=\kappa+\sigma$ of A and B, he manages to synchronize very well. However, in the cryptographic system we propose, such synchronization does not allow the attacker to reliably decode the message.

In our proposed MCPF cryptography system, each laser transmits a signal to the other laser that consists of the original chaotic laser signal with some added low-amplitude message signal. Our simulations show that synchronization is possible even in the presence of the added message. In the Lang-Kobayashi (LK) equations the added message is represented by another term $M_{A/B}(t)$ in the first two equations which is time dependent and different for lasers A and B. The dynamics of laser A are thus given by the following coupled differential equations for the optical field, E, the optical phase Φ, and the excited-state population n:

$$\frac{dE_A}{dt} = \frac{1}{2}G_N n_A E_A(t) + \frac{C_{sp}\gamma[N_{sol}+n_A(t)]}{2E_A(t)} + \kappa E_A(t-)\cos[\omega_0+\Phi_A(t)-\Phi_A(t-)] + \sigma(E_B(t-) + M_B(t-))\cos[\omega_0+\Phi_A(t)-\Phi_B(t-)],$$

$$\frac{d\Phi_A}{dt} = \frac{1}{2}\alpha G_N n_A - \kappa\frac{E_A(t-)}{E_A(t)}\sin[\omega_0+\Phi_A(t)-\Phi_A(t-)] - \sigma\frac{E_B(t-)+M_B(t-)}{E_A(t-)}\sin[\omega_0+\Phi_A(t)-\Phi_B(t-)],$$

$$\frac{dn_A}{dt} = (p-1)J_{th} - \gamma n_A(t) - [\Gamma + G_N n_A(t)]E_A^2(t), \qquad (1)$$

and likewise for laser B. We obtain that for a wide range of values of κ and σ the two lasers achieve stable isochronal synchronization, despite the fact that each laser is receiving an additional and different time-dependent message. This message M_A, sent from A to B, is recovered by laser B via a chaos pass filter procedure, as $\tilde{M}_A$ by subtracting his output from the received input in the manner $\tilde{M}_A=E_A+M_A-E_B$ and then averaged over 1-ns windows, giving the recovered message as $\langle\tilde{M}_A\rangle$. The same method is used by the other laser.

When considering the security of this public cryptographic system we consider a passive attacker who is "listening" to the communication channel and wishes to decipher the secret messages that are transmitted. When the communicating lasers use coupling strength values in the "light gray regime" of Fig. 3, an attacker who uses the same parameters fails to synchronize and hence cannot recover the message correctly. His best chance to synchronize is by adjusting his parameters to the dark gray region in Fig. 3, where he amplifies the coupling signal strength σ and weakens his self-feedback strength κ. In this case he succeeds in synchronizing, as we already explained above, but he still fails to decipher the message. The reason for his failure is that the coupling signal consists both of a fraction of the laser's signal, E, and the message, M, and so the attacker amplifies the message as well as the laser's signal. Hence, the message/signal ratio for the attacker,

$$M \Big/ \left[\left(1+\frac{\kappa_{attacker}}{\sigma_{attacker}}\right)\langle E\rangle\right] \qquad (2)$$

is greater than the message/signal ratio for the parties,

$$M \Big/ \left[\left(1+\frac{\kappa}{\sigma}\right)\langle E\rangle\right] \qquad (3)$$

[19]. This difference in the message/signal ratio causes the attacker to have more errors in his recovered message. Therefore when the attacker amplifies the coupling signal and uses a stronger σ, he does not manage to recover the message to the same extent as the parties and we thus conclude that no matter where in the κ/σ phase space the attacker works, he deciphers the message incorrectly.

Figure 4 displays the traces of the message sent by A, the message recovered by B, and the message recovered by the attacker, for an attacker using a maximal coupling signal σ. One can observe that the attacker's recovered message, although generally following the original message, has several mistakes even in this short sequence. When sending compressed data, even several mistakes can corrupt the entire message. An accepted measure of the ability to recover a message successfully is the bit error rate (BER), the probability of a bit to be decoded erroneously [20].

We measured the BER of the communicating lasers for many different points in the "light gray regime," for which there is a strong self-feedback. For every point we examined we looked for the "best" possible κ,σ values for the attacker, in the entire space (κ,σ) (where the LK equations do not diverge), which gives him the minimal BER value [21]. For all the parameters we checked, the BER of lasers A and B was considerably smaller than the BER of the best attacker. For example

	Example 1	Example 2
κ	80 ns^{-1}	110 ns^{-1}
σ	20 ns^{-1}	40 ns^{-1}
$\frac{M_{A/B}}{\langle E_{A/B}\rangle}$	3%	12%
$\kappa_{attacker}$	30 ns^{-1}	70 ns^{-1}
$\sigma_{attacker}$	90 ns^{-1}	80 ns^{-1}
$\text{BER}_{A/B}$	$\sim10^{-4}$	$\sim10^{-4}$
$\text{BER}_{attacker}$	$\sim10^{-2}$	$\sim10^{-1}$

where $\langle E_{A/B}\rangle$ is the average amplitude of the laser signal and $\kappa_{attacker}$ and $\sigma_{attacker}$ appearing in the table are the values that minimize the BER of the attacker. The added message was changed randomly every 1 ns, giving a rate of 1 Gbit/s. It is clear that the BER of the attacker is few orders of magnitude higher than the BER of the parties. Hence, while a compressed block (for instance, of 10 Kbits) is recovered properly with high probability by the parties, the attacker has many $[O(10^3)]$ error bits. By reducing the transmission rate, for instance, and transmitting a bit every 3 ns (a 1/3 -Gbit/s rate), the BER of the parties can be reduced and the gap between the $\mathrm{BER}_{A/B}$ and $\mathrm{BER}_{attacker}$ is enhanced.

Note that if the two communicating lasers use the same κ and σ as the optimal attacker in the examples above (κ=30 ns^{-1}, σ=90 ns^{-1} or κ=70 ns^{-1}, σ=80 ns^{-1}), they also have BER $\sim 10^{-2}$. Hence working in the light gray regime provides two advantages: the BER in this region is considerably smaller, and the mutual coupling is superior to the unidirectional.

We checked that the synchronization of the mutually coupled lasers is robust under different message signals, such as a "noisy" message, which was also recovered correctly using the MCPF procedure. Finally, we considered an attacker who listens to *both* communication directions, using the coupling signal of both A to B and B to A, and found this attacker to be unsuccessful.

To conclude, we have presented a public-channel cryptographic system, based on two mutually coupled lasers in a MCPF procedure. Encryption security is based on the experimentally demonstrated advantage of mutual coupling over unidirectional coupling. This system is novel in several aspects: It is an optical communication system that is public and does not require a secret key, it enables two-directional message flow, and the security is not limited by a small key space, as in the case of unidirectional CPF. The system proposed here opens a manifold of possibilities: for instance, the extension to generate secret communication among a group of more than two lasers.

[1] I. Fischer, G. H. M. van Tartwijk, A. M. Levine, W. Elsässer, E. O. Göbel, and D. Lenstra, Phys. Rev. Lett. **76**, 220 (1996).

[2] S. Sivaprakasam and K. A. Shore, Opt. Lett. **24**, 466 (1999).

[3] A. Locquet, F. Rogister, M. Sciamanna, P. Megret, and M. Blondel, Phys. Rev. E **64**, 045203(R) (2001).

[4] T. Heil, I. Fisher, W. Elsässer, J. Mulet, and C. Mirasso, Phys. Rev. Lett. **86**, 795 (2001).

[5] A. Hohl, A. Gavrielides, T. Erneux, and V. Kovanis, Phys. Rev. A **59**, 3941 (1999); J. Mulet, C. Masoller, and C. R. Mirasso, *ibid.* **65**, 063815 (2002); J. Javaloyes, P. Mandel, and D. Pieroux, Phys. Rev. E **67**, 036201 (2003); N. Fujiwara, Y. Takiguchi, and J. Ohtsubo, Opt. Lett. **28**, 1677 (2003).

[6] R. Vicente, S. Tang, J. Mulet, C. R. Mirasso, and J. M. Liu, Phys. Rev. E **70**, 046216 (2004).

[7] P. Rees, P. S. Spencer, I. Pierce, S. Sivaprakasam, and K. A. Shore, Phys. Rev. A **68**, 033818 (2003).

[8] L. M. Pecora and T. L. Carroll, Phys. Rev. Lett. **64**, 821 (1990); J.-P. Goedgebuer, L. Larger, and H. Porte, *ibid.* **80**, 2249 (1998); G. D. VanWiggeren and R. Roy, Science **279**, 1198 (1998).

[9] A. Argyris, D. Syvridis, L. Larger, V. Annovazzi-Lodi, P. Colet, I. Fischer, J. Garcia-Ojalvo, C. R. Mirasso, L. Pesquera, and K. A. Shore, Nature (London) **438**, 343 (2005).

[10] I. Fischer, Y. Liu, and P. Davis, Phys. Rev. A **62**, 011801(R) (2000).

[11] N. Gross, W. Kinzel, I. Kanter, M. Rosenbluh, and L. Khaykovich, e-print cond-mat/0604068.

[12] E. Klein, N. Gross, M. Rosenbluh, W. Kinzel, L. Khaykovich, and I. Kanter, e-print cond-mat/0511648.

[13] V. Ahlers, U. Parlitz, and W. Lauterborn, Phys. Rev. E **58**, 7208 (1998); I. V. Koryukin and P. Mandel, *ibid.* **65**, 026201 (2003).

[14] Note that mutually coupled semiconductor lasers are less senstive to a mismatch between their paramters in comparison to unidirectional coupling [11].

[15] Y. Liu, P. Davis, Y. Takiguchi, T. Aida, S. Saito, and J. Liu, IEEE J. Quantum Electron. **39** (2003).

[16] R. Vicente, T. Perez, and C. R. Mirasso, IEEE J. Quantum Electron. **38** (2002).

[17] For the appearance of the second type (generalized synchronization), high coupling intensities are required, which is a disadvantage for the attacker (laser C).

[18] E. Klein, R. Mislovaty, I. Kanter, and W. Kinzel, Phys. Rev. E **72**, 016214 (2005).

[19] If the attacker wishes to keep the same message/signal ratio $\frac{\kappa_{attacker}}{\sigma_{attacker}}=\frac{\kappa}{\sigma}$, then if κ and σ are in the light gray regime of Fig. 3, so must be $\kappa_{attacker}$ and $\sigma_{attacker}$.

[20] Note that minimizing the BER or maximizing the synchronization are in general two different tasks. Minimizing the BER, for instance, requires that the average recovered signal over a window have the same sign as the message, while the local synchronization can be reduced.

[21] Since we are working in the LFF regime, we excluded the downfalls from the BER calculation (for all lasers), since during the downfalls the lasers temporarily fall out of synchronization.