Available online at www.sciencedirect.com
SCIENCE DIRECT®
C. R. Physique 5 (2004) 643–656
COMPTES RENDUS PHYSIQUE

Cryptography using optical chaos/Cryptographie par chaos optique

Synchronization of chaos in microchip lasers and its communication applications

Atsushi Uchida [a,b,*], Shigeru Yoshimori [a]

[a] *Department of Electronics and Computer Systems, Takushoku University, 815-1 Tatemachi, Hachioji, Tokyo 193-0985, Japan*
[b] *Institute for Research in Electronics and Applied Physics, University of Maryland, College Park, MD 20742, USA*

Available online 17 June 2004

Presented by Guy Laval

Abstract

We overview some experimental and numerical demonstrations on the synchronization of chaos and its communication applications using Nd:YVO_4 microchip solid-state lasers. Synchronization of chaos is achieved with several coupling configurations. Several encoding and decoding schemes for communication applications are also demonstrated by using the synchronization of chaos in microchip lasers. A new approach to secure communications using chaos based on information theoretic security is introduced. ***To cite this article: A. Uchida, S. Yoshimori, C. R. Physique 5 (2004).***

Résumé

Synchronisation de chaos dans les micro-lasers et ses applications aux communications. Nous passons en revue une démonstration expérimentale et numérique de synchronisation entre dynamiques chaotiques produites dans des micro-lasers solide Nd :YVO_4 ; une application de cette synchronisation aux communications est étudiée. Différentes configurations de couplage sont discutées. Nous démontrons également plusieurs schémas de codage et décodage utilisant des micro-lasers en régimes chaotiques synchronisés à des fins de communication. Enfin, une nouvelle approche cryptographique utilisant les dynamiques chaotiques est proposée, dont la sécurité est discutée à partir d'éléments de théorie de l'information. ***Pour citer cet article : A. Uchida, S. Yoshimori, C. R. Physique 5 (2004).***

Keywords: Synchronization; Chaos; Communication; Microchip laser; Security; Encoding; Decoding; Information theory

Mots-clés : Synchronisation ; Chaos ; Communication ; Micro-laser ; Sécurité ; Codage ; Décodage ; Théorie de l'information

1. Introduction

Optical communication systems that use chaos synchronization have attracted increasing interest since the first experimental demonstration was reported in 1998 [1–3]. The use of chaos for communication applications may have a potential to guarantee privacy for signal transmission. Chaos can be used as a random code (e.g., one-time pad) to conceal the original message. Synchronization of chaos is an essential technique for sharing an identical chaotic waveform as the common random code in both a transmitter and a receiver for signal decoding.

* Corresponding author.
E-mail addresses: a-uchida@es.takushoku-u.ac.jp (A. Uchida), yosimori@es.takushoku-u.ac.jp (S. Yoshimori).

1631-0705/$ – see front matter
doi:10.1016/j.crhy.2004.05.001

The privacy in chaos communications relies on the fact that one may not be able to reproduce the chaotic temporal waveforms of the laser output without synchronizing two lasers or without knowing the matching parameter values between the transmitter and the receiver. The tolerance of synchronization regions against parameter mismatch between the transmitter and the receiver is one of the important factors in measuring the privacy in chaotic communication systems. There is always a trade-off between the difficulty of synchronization and the privacy, because higher privacy is guaranteed by narrower parameter ranges where synchronization is achieved. These hardware-oriented security systems using chaos could be promising techniques in the near future.

Solid-state lasers are reasonable tools to test the fundamental physics of synchronization of chaos in laser systems. A solid-state laser that has a short cavity length less than one millimeter is specifically called a microchip laser. Since the short cavity length allows a few longitudinal modes in the laser cavity to oscillate, it is easy to model the dynamics of microchip lasers precisely. The relaxation oscillation frequency of microchip lasers is around a few MHz, which is much less than the relaxation oscillation frequency of semiconductor lasers, around a few GHz. This low-frequency feature allows one to detect chaotic temporal waveforms easily in experiment without using high-speed detection equipments. From the dynamical point of view, the dynamics of microchip lasers are relatively simple compared with semiconductor lasers, because there is no coupling effect between the electrical amplitude and the optical phase in the laser cavity, which is referred to as the α parameter in semiconductor lasers. Solid state lasers are also good tools to test communication schemes using the synchronization of chaos. Solid state lasers can be used for optical communications in space, because the optical frequency of solid-state lasers is much more stable than that of semiconductor lasers.

In this article, we overview some experimental and numerical demonstrations on the synchronization of chaos, and its communication applications by using Nd:YVO_4 microchip solid-state lasers. Chaos synchronization can be categorized into two coupling schemes: a one-way coupling and a mutual coupling. In this paper, we discuss chaos synchronization only in a one-way coupling scheme, which is well suited for communication purposes, to connect distantly separated chaotic lasers and to maintain the original chaotic carriers. We show synchronization of chaos with several coupling configurations. Several encoding and decoding schemes for communication applications are also demonstrated by using the synchronization of chaos in microchip lasers. A new approach to secure communications using chaos based on information-theoretic security is introduced.

The following sections in this paper are arranged as follows. Section 2 contains the demonstration of chaos synchronization in several coupling configurations. The characteristics of chaos synchronization are described for each coupling scheme. Section 3 gives two demonstrations of message encoding and decoding with synchronized chaotic microchip lasers for the purpose of communication applications. Section 4 contains a new scheme for chaos communications without using synchronization. A generation of information-theoretic secure keys is demonstrated experimentally. Finally, we conclude these results in Section 5.

2. Synchronization of chaos in microchip lasers

2.1. Coherent coupling

One of the simplest coupling methods for chaos synchronization is a coherent coupling between the electrical fields of two lasers. When the output from one of the two lasers is injected into the other laser cavity, synchronization can be achieved. Since the two lasers are coupled through the complex electrical fields of the two lasers, the matching of optical frequency and phase is crucial for the achievement of chaos synchronization. Injection locking is a useful technique to match the optical frequency between two lasers [4]. In this subsection, we describe the experimental demonstration of the synchronization of chaos in two coherently coupled microchip lasers in a one-way coupling configuration [5,6].

Fig. 1 shows the experimental setup. Two Nd:YVO_4 microchip lasers (wavelength $\lambda = 1064$ nm) pumped by laser diodes ($\lambda = 809$ nm) were used as laser sources. The laser oscillated with 1–3 longitudinal modes depending on the pumping power. The pumping power was set to 1.7 with respect to threshold to maintain single longitudinal-mode oscillations. Chaotic outputs in microchip lasers were obtained by modulating the pumping power around the frequency of the sustained relaxation oscillation of 1.38 MHz in this experiment. When pump modulations were applied to both of the microchip lasers with a modulation frequency of 1.34 MHz and with a modulation depth of 18%, individual chaotic pulsations were obtained. The dynamics of microchip lasers are described by the Tang–Statz–deMars equations, in which the spatial hole burning effect in the laser crystal is taken into account [7]. Chaotic dynamics in microchip lasers have been intensively investigated in [8,9].

A fraction of the master laser output was unidirectionally and coherently coupled to the slave laser cavity for chaos synchronization. The optical frequencies of the two microchip lasers were precisely controlled with thermoelectronic coolers. The achievement of synchronization of chaos is highly dependent on the injection locking effect, where the optical frequencies of two individual lasers can be perfectly matched when the frequency difference is set within a certain injection-locking range [4]. We adjusted the temperature of the laser crystal of the two lasers so that the difference of the two optical frequencies was within the injection locking range of 200 MHz.

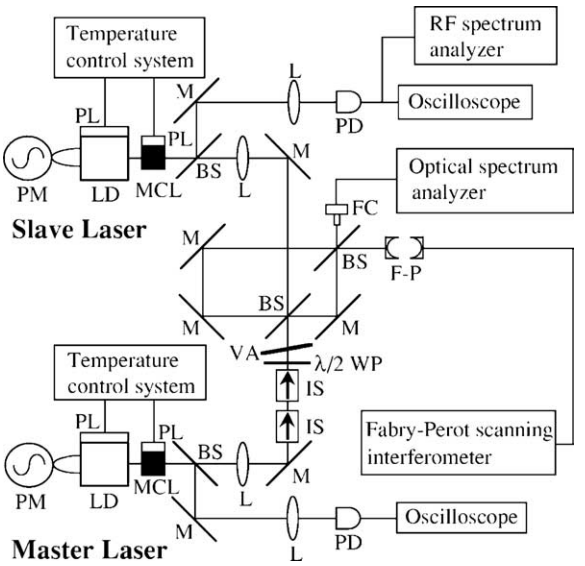

Fig. 1. Experimental setup for chaos synchronization in two Nd:YVO_4 microchip lasers with pump modulation. BS, beam splitter; L, lens; M, mirror; VA, variable attenuator; LD, laser diode; MCL, Nd:YVO_4 microchip laser; PL, Peltier device; IS, optical isolator; PD, photodiode; FC, fiber coupler; PM, pump modulation; $\lambda/2$ WP, $\lambda/2$ wave plate; F–P, Fabry–Pérot étalon.

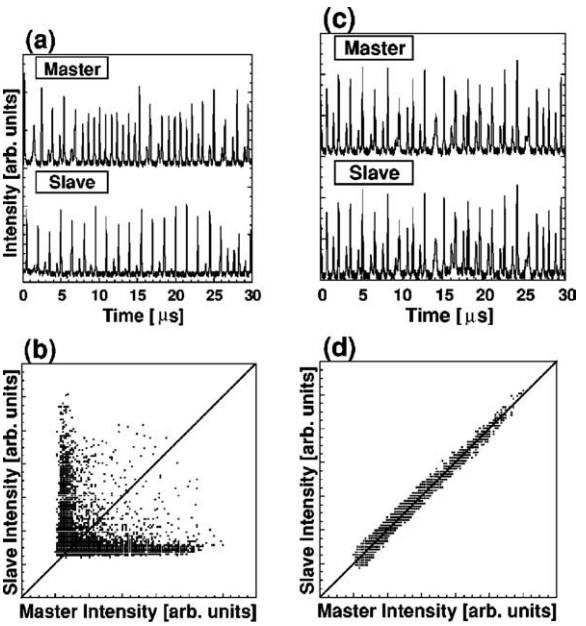

Fig. 2. Experimentally obtained chaotic temporal waveforms and correlation plots for the two laser outputs: (a), (b) without synchronization and (c), (d) with synchronization.

Fig. 2 shows the chaotic temporal waveforms and the correlation plots between the two laser outputs. There is no correlation at all between the chaotic pulsations in the two lasers without coupling as shown in Figs. 2(a) and 2(b). When a fraction of the master laser output is injected into the slave laser cavity and injection locking is achieved between the two lasers, the chaotic oscillations are synchronized as shown in Fig. 2(c). The linear correlation between the two laser outputs shown in Fig. 2(d) exhibits synchronization. This synchronization can be maintained for tens of hours, as long as the injection locking of the two laser frequencies is retained.

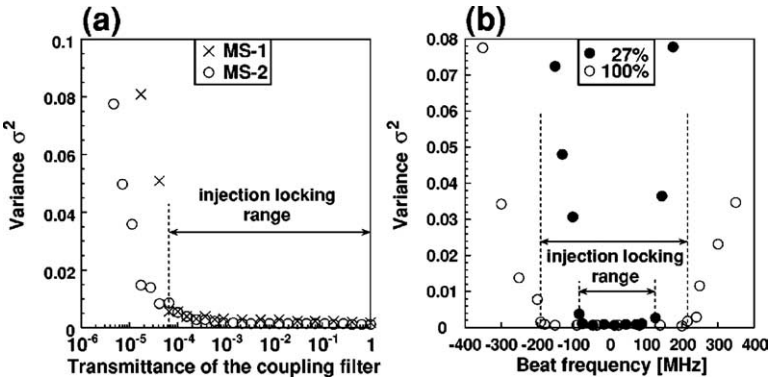

Fig. 3. Variances of the correlation plots as functions of (a) injection power and (b) beat frequency between the two optical frequencies. The arrows indicate the injection-locking range.

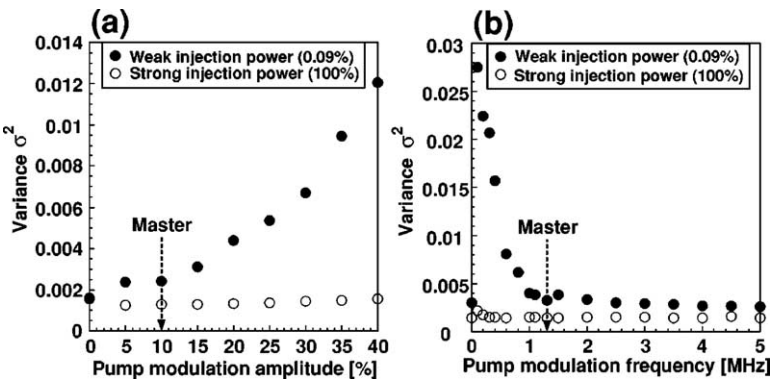

Fig. 4. Variances of the correlation plots as functions of (a) amplitude and (b) frequency of the pump modulation in the slave laser. Solid circles, weak injection power; open circles, strong injection power. The downward arrows indicate parameter matching between the master and slave lasers.

To evaluate the quantitative accuracy of chaos synchronization, the variance σ^2 of the normalized correlation plot from a best-fit linear relation is used, which is defined as

$$\sigma^2 = \frac{1}{N}\sum_{i}^{N}(I_{\mathrm{m},i} - I_{\mathrm{s},i})^2, \tag{1}$$

where N is the total number of sampling points of the temporal waveforms and $I_{\mathrm{m},i}$ and $I_{\mathrm{s},i}$ are the normalized intensities of the master and slave lasers at the i-th sampling point. A smaller variance σ^2 implies higher accuracy of chaos synchronization. Fig. 3(a) shows the variances of the correlation plots as a function of injected power from the master to the slave lasers. The injection power is altered with a variable attenuator. It is found that the accuracy of synchronization is always quite high at any injection power higher than the threshold for injection locking. Above the threshold, relatively constant variances are maintained as the injection power increases. Fig. 3(b) shows the variances of the correlation plots as a function of the beat frequency at two constant injection powers. The temperature of the slave crystal is slightly shifted, which causes detuning. Low and constant variances are maintained within the injection locking range. From Figs. 3(a) and 3(b), it is found that the synchronization range coincides with the injection locking range.

The accuracy of synchronization is investigated when one of the parameters for chaos generation is mismatched between the two lasers. The amplitude or the frequency of the pump modulation in the slave laser is slightly shifted from that in the master laser. Fig. 4 shows variances as functions of the amplitude and frequency of the pump modulation in the slave laser under weak and strong injection powers. With weak injection power (solid circles in Fig. 4), the variance gradually changes as the modulation parameter is changed. It is worth noting that matching of the modulation parameters is not required to achieve accurate synchronization. Moreover, a high accuracy is always maintained with strong injection power (open circles in Fig. 4), regardless of the values of the modulation parameters. These results imply that intense injection of the master laser can suppress

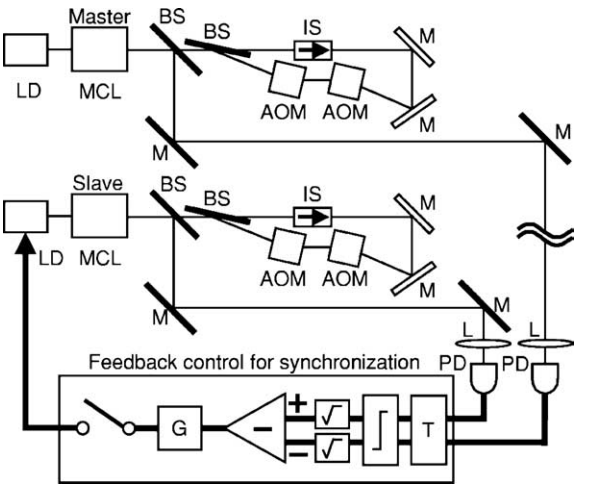

Fig. 5. Model of the incoherent feedback method for chaos synchronization in microchip lasers: AOM, acousto-optic modulator; BS, beam splitter; G, electronic amplifier for gain; IS, optical isolator; L, lens; LD, laser diode for pumping; M, mirror; MCL, microchip laser; PD, photodiode; T, time delay.

the original dynamics in the slave laser, and the accuracy of synchronization is independent of the mismatch of the pump modulation between the master and slave lasers.

From these investigations, the principle of synchronization of chaos in coherently coupled lasers can be interpreted as the regeneration of the envelope of the chaotic laser output through the mechanism of injection locking. For multi-mode lasers, synchronization of chaos requires frequency locking of all the corresponding longitudinal modes between two coherently coupled lasers, according to [5].

2.2. Incoherent feedback

In the case of coherent coupling, the achievement of chaos synchronization is strongly dependent on the matching of the fast optical frequency by using injection locking. Therefore, it would be easy to reproduce the chaotic waveforms of the transmitter by using unauthorized lasers without knowing the parameter values of the transmitter laser, when eavesdroppers can achieve injection locking between the transmitter laser and their own lasers only by tuning the optical frequency. Moreover, this coherent synchronization scheme cannot be applied to conventional optical communication systems, where it does not need to match the optical frequency between the transmitter and receiver lasers. Therefore, it is important to develop a synchronization technique that is not dependent on optical frequency (phase) for applications of optical communications.

In this subsection, we describe a chaos-synchronization method using 'incoherent' (independent of the optical phase or frequency) feedback [10] to achieve a synchronization that is independent of the injection locking effect and that satisfies narrow parameter regions for synchronization against parameter mismatch. In this method, two signals of the laser intensity for the master and slave lasers are detected simultaneously, and the amount of feedback-control signal from the subtraction of the two detected signals is calculated. The feedback is applied to the pumping power of the microchip laser in the slave laser. Chaotic dynamics of population inversion in the two lasers are thus synchronized by using the feedback signal calculated from the detected laser intensities.

Fig. 5 shows the concept of the incoherent feedback method for chaos synchronization in microchip lasers. Chaotic pulsations of the output are generated in two microchip lasers with two acousto-optic modulators (AOM) in single-longitudinal-mode operation, and the outputs of the two lasers are independently detected by two photodiodes. The peak heights of the pulses are stored in memory and used for calculation in a computer. When the duration between the two pulses is within a certain time T_{th} and the difference of peak heights is within a certain value E_{th}, a control signal is applied to the pumping power of the slave laser for a certain duration T_{c} just after the latter pulse. The value of the control signal is proportional to the difference between the peak heights of the square root of the laser intensities (i.e., electrical field $E = \sqrt{I}$). This control procedure is described as follows:

$$w_{\mathrm{s}} = w_{\mathrm{s},0} + G\bigl(\sqrt{I_{\mathrm{p,s}}} - \sqrt{I_{\mathrm{p,m}}}\bigr) \quad \text{for } T_{\mathrm{c}} \tag{2}$$

$$\text{if } |T_{\mathrm{p,s}} - T_{\mathrm{p,m}}| < T_{\mathrm{th}} \quad \text{and} \quad \bigl|\sqrt{I_{\mathrm{p,s}}} - \sqrt{I_{\mathrm{p,m}}}\bigr| < E_{\mathrm{th}},$$

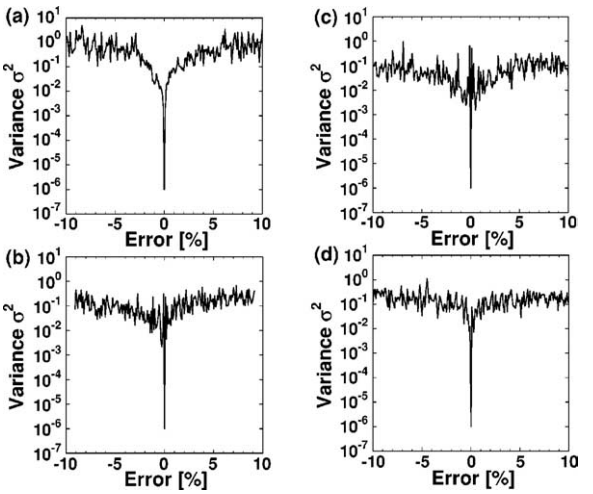

Fig. 6. Accuracy of chaos synchronization (variance σ^2) as a function of parameter mismatch: (a) pumping power, (b) ratio of lifetimes of the population inversion and photon in the cavity, (c) modulation amplitude of the AOM, and (d) modulation frequency of the AOM.

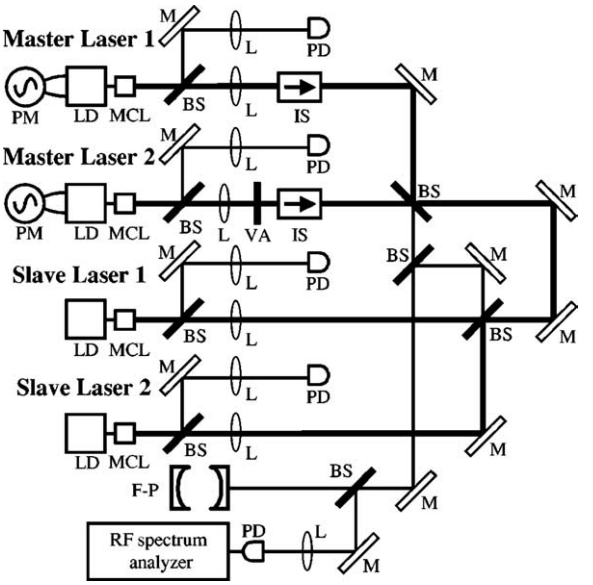

Fig. 7. Experimental setup for dual synchronization of chaos. BS, beam splitter; F–P, Fabry–Perot interferometer; IS, optical isolator; L, lens; LD, laser diode for pumping; M, mirror; MCL, Nd:YVO_4 microchip laser; PD, photodiode; PM, pump modulation; VA, variable attenuator.

where w_s is the pumping power of the slave laser, $w_{s,0}$ is the constant pumping power, G is the feedback gain, $I_{p,s}$ and $I_{p,m}$ are the peak heights of the detected chaotic pulses in the slave and master lasers, $T_{p,s}$ and $T_{p,m}$ are the measured times corresponding to the pulse peak in the slave and master lasers, respectively. In this method the difference of peak intensities between the two lasers is fed back to the dynamics of population inversion through the pumping power. It should be noted that there is a linear relationship between the peak height of electrical pulsations and the decrease of population inversion. Synchronization of chaos is achieved at certain values of the gain ($0.5 < G < 1.2$) [10].

The regions of chaos synchronization against parameter mismatch between the two microchip lasers were quantitatively investigated for various internal parameters by numerical calculations. One of the parameters in the slave laser was fixed and the corresponding parameter in the slave laser was slightly shifted. Other parameters were set to be identical for the two lasers. Fig. 6 shows the accuracy of synchronization (variance σ^2) as functions of parameter mismatch of the pumping power, the ratio of lifetimes of the population inversion and photon in the cavity, the modulation amplitude of the AOM, and the modulation frequency of the AOM. It is found that synchronization is easily destroyed when the parameter mismatch is increased by

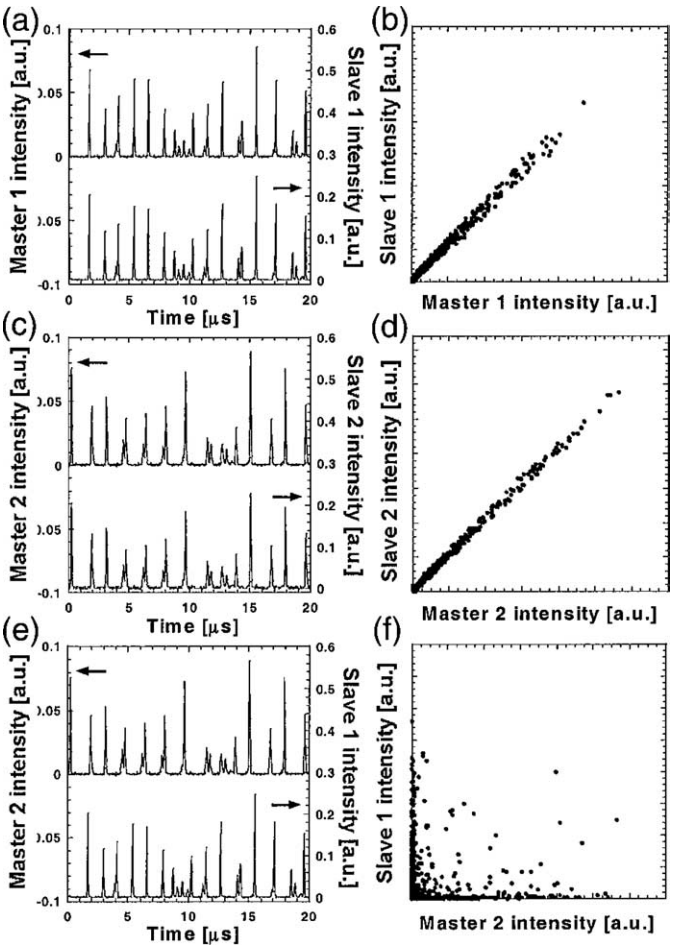

Fig. 8. Temporal waveforms and their correlation plots for the $M1$–$S1$ [(a), (b)], $M2$–$S2$ [(c), (d)], and $M2$–$S1$ [(e), (f)].

more than 1% for all the laser parameters. The synchronization regions obtained by the incoherent feedback method are much smaller than those obtained by the coherent coupling method shown in Fig. 4. Since the same dynamics of population inversions between the two lasers are required in this method, all the laser parameters must be carefully matched to each other for precise synchronization. These results imply that the difficulty in imitating synchronizing lasers is greatly increased by using this incoherent feedback method, which might be useful for applications of secure optical communications.

Synchronization of chaos was also demonstrated in Nd:YAG microchip lasers with optoelectronic feedback in [11]. Generalized synchronization of chaos is observed when the microchip laser has two-longitudinal-mode oscillations. Since the lumped signal applied to the response laser through optoelectronic feedback does not contain any details of the individual mode dynamics, generalized synchronization is observed instead of identical synchronization [11].

2.3. Dual synchronization of chaos

Many studies on the synchronization of chaos have been reported so far in a single pair of one-way coupled laser systems for the purpose of optical communications. However, it is necessary to investigate synchronization of chaos in multiple pairs of lasers for multi-user communication systems. Multiplexing chaos using synchronization has been numerically achieved in a simple map and delay-differential equations [12,13]. To synchronize each pair of chaotic systems, all the parameter settings must be identical between the transmitter and the receiver, whereas they must be slightly shifted between different pairs of chaotic systems. Synchronization of chaos between two pairs of chaotic systems is particularly called ‘dual synchronization of chaos’ [13].

In this subsection, we describe the experimental demonstration of dual synchronization of chaos in two pairs of Nd:YVO_4 microchip lasers in a coherent coupling configuration over one transmission channel, [14,15]. The optical frequency of each

laser is changed and the condition of injection locking is controlled to achieve dual synchronization between the corresponding pairs in the transmitters and the receivers.

Fig. 7 shows the experimental setup for the dual synchronization of chaos. Two of the microchip lasers were used as master lasers, which were referred to as '$M1$' for master laser 1 and '$M2$' for master laser 2. The other two lasers were used as slave lasers ('$S1$' for slave laser 1 and '$S2$' for slave laser 2). For $M1$ and $M2$, the injection current of a laser diode used for pumping was sinusoidally modulated to obtain chaotic pulsation. A fraction of the master laser outputs was mixed at a beam splitter and propagated through one-transmission channel in a free space (the thick solid line in Fig. 7). The combined signals of $M1$ and $M2$ were injected into the two slave laser cavities for dual synchronization.

The temperatures of $M1$ and $M2$ were adjusted to obtain injection locking between the optical frequencies of a pair of $M1$ and $S1$ (referred to as '$M1$–$S1$'), and a pair of '$M2$–$S2$' by monitoring the spectra on the Fabry–Perot scanning interferometer. When two of the beat frequencies for $M1$–$S1$ and $M2$–$S2$ were adjusted within the injection-locking range, the two beat frequencies disappeared and the two laser frequencies in each pair for $M1$–$S1$ and $M2$–$S2$ were perfectly matched. The injection locking was achieved only for $M1$–$S1$ and $M2$–$S2$, not for the other coupling combinations.

Fig. 8 shows the temporal waveforms and their correlation plots for the $M1$–$S1$, $M2$–$S2$, and $M2$–$S1$. Synchronization of chaos is achieved between the corresponding pairs of $M1$–$S1$ and $M2$–$S2$ independently under injection locking, whereas it is not achieved for $M2$–$S1$. The $S1$ laser reproduces the $M1$ component separately from the injection signal of the combination of $M1$ and $M2$. The output of $S2$ is also synchronized with only the $M2$ component although the combined signal of $M1$ and $M2$ is injected. Therefore, dual synchronization of chaos is achieved in two pairs of microchip lasers. The numerical calculations in [14] suggest that the dynamics of injection locking are crucial for the achievement of dual synchronization of chaos in coherently coupled lasers, as well as the case of single pair of coherently coupled lasers.

3. Communication with chaotic microchip lasers

3.1. Classification

The methods for achieving chaos communication by use of lasers can be classified into the following types [16]: chaotic masking [17–20], chaotic modulation [1–3], and chaos shift keying [21]. Chaotic masking is a simple encoding scheme in which a message signal is added or multiplied on a chaotic carrier that is independent of the message. The message is recovered by subtracting or dividing the synchronized chaotic signal in the receiver from the transmitted signal. The message has to be small enough so that the original chaotic carrier can be regenerated in the receiver via synchronization. Chaotic modulation is a dynamical encoding method in which the message modulates chaotic dynamics in the transmitter. The modulated chaotic signal is directly injected into the receiver in order to generate the original chaotic waveform. When this method is applied to time-delayed chaotic systems and the message is encoded inside the time-delay loop, perfect message recovery can be achieved regardless of the amount of the message. Chaos shift keying is a digital modulation method based on two different chaotic states. Depending on the current value of the digital bits of '0' or '1', the signal from one of two chaos generators with different characteristics is transmitted. There are also two chaos generators in the receiver whose parameter values are matched to those of the corresponding generators in the transmitter. The message bits can be determined by knowing which chaotic generator in the receiver is synchronized with the transmission signal. Chaotic on-off keying is a special case of chaos shift keying. It requires only one chaotic generator in the receiver whose parameter values are matched to those of one of the two generators in the transmitter. The binary bits can be determined by checking whether synchronization is achieved or not in the receiver.

3.2. Chaotic masking with a digital message

In this subsection, we describe the experimental demonstration of the chaotic masking method with a digital message in coherently coupled microchip laser systems in [22]. Fig. 9 shows the experimental setup for signal transmission. Two Nd:YVO_4 microchip lasers pumped by laser diodes were used. Chaotic outputs of the microchip lasers were obtained by modulation of the injection current of the laser diode in the transmitter. The chaotic output of the microchip laser was externally modulated with an acousto-optic modulator (AOM) with a sinusoidal periodic wave at a frequency of 4.0 MHz and a depth of 0.2%. The modulation of the AOM was turned on and off at a frequency of 0.1 MHz to encode a sequence of digital bits in the laser output as a message signal. Chaotic oscillations created by turning the AOM on and off were regarded as binary signals 1 and 0, respectively. The laser output with a message was transmitted to the receiver in a free space and injected into the laser cavity in the receiver for chaos synchronization. The chaotic laser outputs of the transmission signal (chaos + digital message) and the receiver (synchronized chaos) were measured simultaneously with a digital oscilloscope and the original binary message was decoded by subtraction of these two signals.

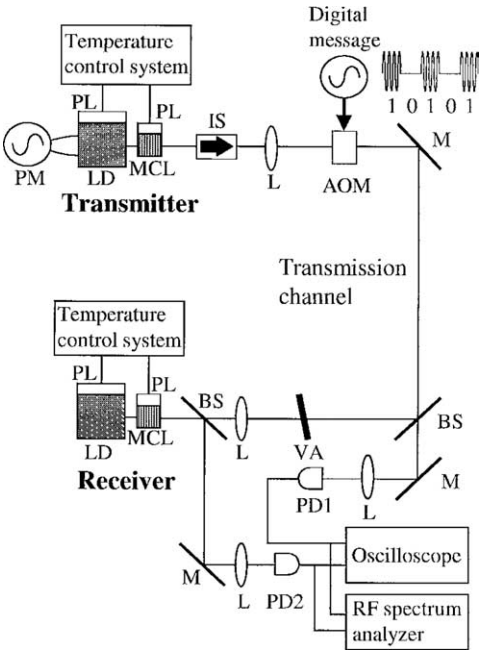

Fig. 9. Experimental setup for the transmission of a digital message based on the chaotic masking method. AOM, acousto-optic modulator; BS, beam splitter; L, lens; M, mirror; VA, variable attenuator; LD, laser diode; MCL, Nd:YVO_4 microchip laser; PL, Peltier device; IS, optical isolator; PD, photodiode; PM, pump modulation.

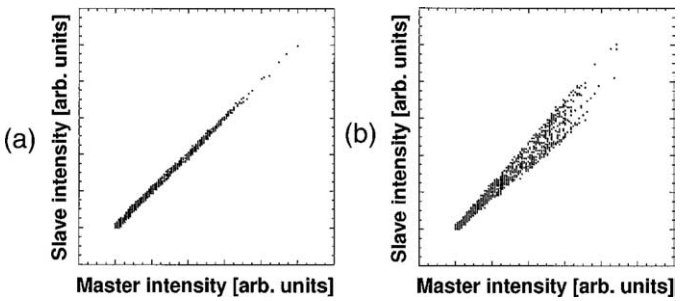

Fig. 10. Correlation plots between waveforms of the two laser outputs (a) without and (b) with external modulation by the AOM.

Fig. 10 plots the correlation between waveforms of the transmission signal and synchronized signal in the receiver for the cases of without and with the external modulation by the AOM. Accurate synchronization is achieved only when the external modulation is switched off, as shown in Fig. 10(a). This state corresponds to binary signal 0. Synchronization is achieved with slightly degraded accuracy in the presence of the external modulation owing to a change in the optical intensity through the AOM, as shown in Fig. 10(b). This state corresponds to binary signal 1. The digital message encoded by the AOM can be easily distinguished by knowing the accuracy of chaos synchronization.

Fig. 11(a) shows the results of message recovery. Message components cannot be observed in the output of the transmitter and the receiver in Figs. 11(a) and 11(b). When the two laser outputs are normalized and one is subtracted from the other, the message can be obtained as an envelope of chaotic oscillation, as shown in Fig. 11(d). The original messages can be recovered by filtering the difference of the two outputs with a low-pass filter. The digital sequence clearly appears in Fig. 11(e), and the binary bits can be judged according to a certain threshold value.

3.3. Chaotic masking with an analog message

In this subsection, we describe the numerical demonstration of the recovery of an analog message signal embedded in a chaotic carrier by using the chaotic masking method in coherently coupled microchip lasers [19]. An AOM is used to encode an analog message (a sinusoidal wave) by modulating the intensity of a chaotic laser output (the same configuration in Fig. 9). The

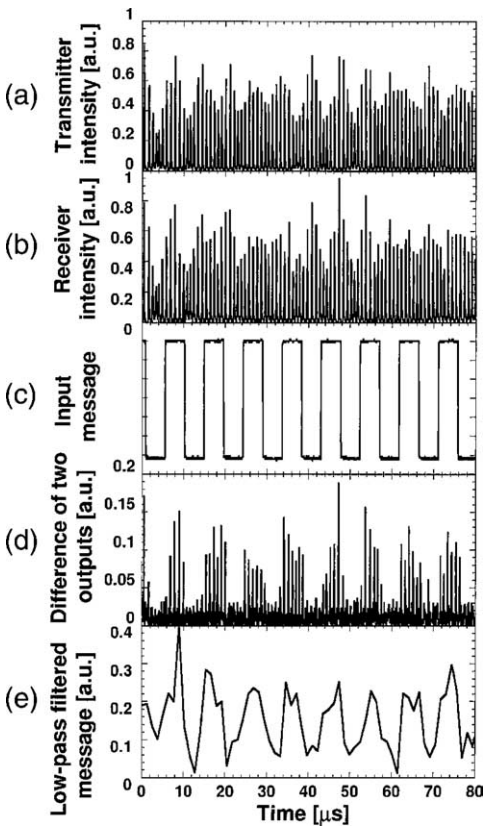

Fig. 11. (a) Temporal waveform of the transmitter output with a digital message, (b) temporal waveform of the synchronized receiver output, (c) encoded digital message, (d) absolute value of the difference between the two normalized laser outputs of (a) and (b), (e) decoded temporal waveform with a low-pass filter from the signal in (d).

modulation amplitude and frequency are set to 10% and 0.1 MHz, respectively. At a receiver, one detects both the transmission signal and the synchronized output of the receiver laser. The message can be recovered by dividing the transmission signal including the chaos and message components by the synchronized outputs of the slave laser.

Fig. 12 shows temporal waveforms for the transmission signal, the slave laser output, the division of these two signals, and the corresponding rf spectra. A message component cannot be clearly observed in the temporal waveform of the transmission signal (Fig. 12(a)). However, the message component is recovered by dividing the transmission signal by the synchronized output of the slave laser as shown in Fig. 12(c). In the rf spectrum of the transmission signal in Fig. 12(d), a chaotic broadband spectrum is observed with the message component at 0.1 MHz and the pump modulation for generating chaos at 1.08 MHz. However, the message component decreases in the rf spectrum of the synchronized output as shown in Fig. 12(e). The spectral peak corresponding to the message component (0.1 MHz) can be extracted by dividing these two spectra, as clearly seen in Fig. 12(f).

As Fig. 12 shows, the effect of peak reduction in the spectrum of the slave laser can be most clearly seen when the amplitude of the modulation signal is large enough for the peak to be outstanding in the broad spectrum of the transmitted signal. We emphasize that this effect holds for when the modulation signal is small, and comparable in power to the neighboring chaos components, as would be required for effective masking.

The ratio of the heights of the spectral peaks corresponding to the message component for the two lasers was calculated, which is referred to as the amplitude transfer function. A smaller amplitude transfer function implies higher recovery of the message component. Fig. 13 shows the amplitude transfer function for periodic modulation imposed on the chaotic carrier as a function of the modulation frequency (open circles in Fig. 13). When the modulation frequency is set at approximately the relaxation oscillation frequency ($\sim$1.0 MHz), the peak heights of the message components are the same between the transmitter and the receiver (i.e., the amplitude transfer function is 1), which implies that the message recovery has failed. On the other hand, the amplitude transfer function decreases as the modulation frequency is decreased lower than the relaxation oscillation frequency. Therefore, message recovery can succeed at a lower modulation frequency than the relaxation oscillation frequency.

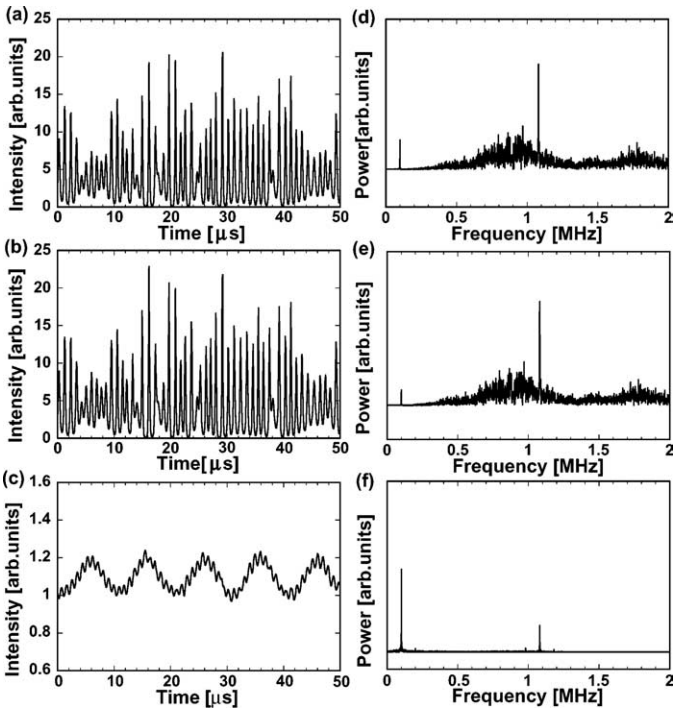

Fig. 12. Temporal waveforms for (a) transmission signal, (b) slave laser output, (c) division of the two signals of (a) and (b). (d), (e), and (f) are the corresponding rf spectra of (a), (b), and (c), respectively.

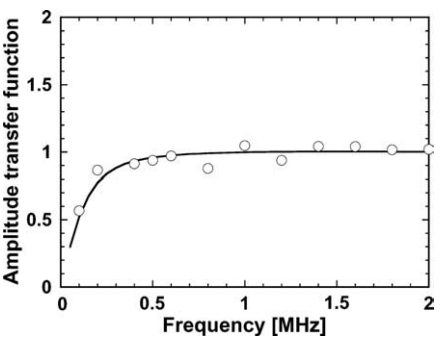

Fig. 13. Amplitude transfer function for the periodic modulation imposed on the chaotic carrier (open circles) and on the stable carrier (solid curve).

This feature can also be seen in the modulated microchip laser with steady state output (the solid curve in Fig. 13). These frequency characteristics of the message component are very similar to those observed in semiconductor lasers [20].

4. New trend of communications with chaotic lasers

4.1. Information theoretic security

As pointed out in the introduction, the security of communication schemes with chaos relies on the robustness of chaos synchronization against parameter mismatch. There is always a trade-off between the difficulty of synchronization and privacy, because higher privacy is guaranteed by narrower parameter ranges where synchronization is achieved. To overcome this issue, communication schemes not using chaos synchronization may be useful. One of the new approaches to secure communications with chaos is a secure key generation based on information theory, proposed by Uchida, Davis, and Itaya [23]. Information-

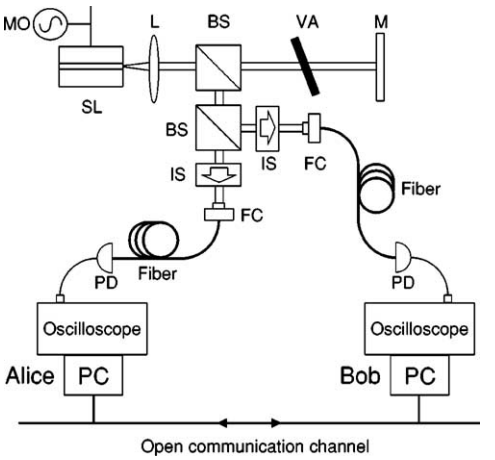

Fig. 14. Experimental setup for secure key generation. The random signal source is a semiconductor laser with optical feedback. The output from the laser is sent to two separate receivers, which record independent random samples of the signal. BS, beam splitter; FC, fiber coupler; IS, isolator; L, lens; M, mirror; MO, modulation for trigger; PC, personal computer; PD, photodetector; SL, semiconductor laser; VA, variable attenuator.

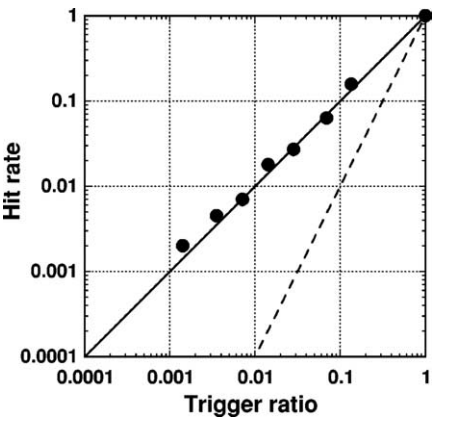

Fig. 15. Data hit rate (R_{hit}) of the sampled data as a function of the trigger-acquisition time ratio (R_{ta}). The solid dots indicate the experimental data of the hit rate between Alice and Bob. The solid line indicates the expected theoretical line for the number of Alice–Bob hits ($R_{\text{hit}} = R_{\text{ta}}$). The dashed line indicates the theoretical line for the number of Alice–Bob hits that are also expected for Eve ($R_{\text{hit}} = (R_{\text{ta}})^2$).

theoretic security is based on probability theory and on the fact that an adversary's information is limited. One approach to information theoretic security assumes that there is a public source of randomness and that all parties have limited storage so that they cannot record all randomness from the source. One may use a physically chaotic semiconductor laser operating in the gigahertz regime in order to satisfy this assumption. This method does not require synchronization between two chaotic lasers and the degree of security can be estimated quantitatively.

This information-theoretic secure-key generation scheme is described as follows (Fig. 14) [23]. Two nodes, Alice and Bob, wish to share keys which are secure with respect to an eavesdropper, Eve. Alice and Bob independently sample the random signal from a chaotic semiconductor laser, and then use an open communication channel to exchange information about which samples they acquired. From listening to the exchange between Alice and Bob on the open channel, Eve also learns which samples Alice and Bob have recorded. However, since the content of the samples is not revealed on the open channel, and the exchange on the open channel only takes place after the transmission from the random signal source is finished, Eve cannot know the keys constructed by Alice and Bob unless she had already acquired the corresponding samples *before* Alice and Bob revealed which samples they have. Such samples can be used to make a secure key if no one can record the whole random signal and the probability of Eve coincidentally acquiring the same samples as both Alice and Bob is sufficiently small.

Let us consider the chances of Alice and Bob acquiring the same samples. The chances of acquiring the same waveform is defined as the hit rate, $R_{\text{hit}} = N_{\text{hit}}/N_{\text{data}}$, where N_{hit} is the number of coincident waveforms and N_{data} is the total number of waveforms acquired in one session. The essential limiting feature of the acquisition system is that it requires a certain acquisition time T_{acq} with a random jitter to record the waveform and prepare for the next grab. The trigger period T_{trg} is set to be shorter than the acquisition time T_{acq} to guarantee that sampling is incomplete. Furthermore, if the trigger period is less than the jitter range, then subsequent samples by Alice and Bob become statistically independent, and one can then expect R_{hit} to be proportional to the trigger-acquisition time ratio $R_{\text{ta}} = T_{\text{trg}}/T_{\text{acq}}$. Fig. 15 shows how the hit rate changes as the trigger-acquisition time ratio R_{ta} is changed from 1 to 10^{-3}, at 10^3 samples per session. The solid dots indicating the experimental data of the hit rate between Alice and Bob agree well with the anticipated theoretical line $R_{\text{hit}} = R_{\text{ta}}$. The dashed line in Fig. 15 indicates the theoretical line for the number of Alice–Bob hits that are also expected for Eve, which is $R_{\text{hit}} = (R_{\text{ta}})^2$. As R_{ta} is decreased, the difference between the solid and dashed lines increases, showing the smaller ratio of samples expected to be acquired by Eve. The security of the system relies on this probability being sufficiently small [23].

Alice and Bob can increase the security of keys by combining all the N_{hit} common samples found in one session into a single common key. This is one of the methods of 'privacy amplification' which can be used if Eve can accidentally acquire some but not all of the keys. The chance of Eve of getting all the N_{hit} common Alice–Bob samples needed to make this combined key is

$(R_{\rm ta})^{N_{\rm hit}}$. For the session length of the experiment in Fig. 15, this chance for Eve is only 10^{-100} in the case of $R_{\rm ta} = 10^{-1}$ and $N_{\rm hit} = 100$.

Information-theoretic security avoids the reliance on un-proven assumptions about the complexity of computations, and is 'future-proof' in the sense that the security of keys generated today will not be compromised by improvements in computing technology, including quantum computing, in the future.

5. Conclusion

We have reviewed the three schemes of synchronization of chaos in microchip lasers in one-way coupling configurations for communication applications. In the coherent coupling scheme the laser light of the transmitter is directly injected into the laser cavity in the receiver. Synchronization of chaos is achieved under the condition of injection locking. In the incoherent coupling scheme two signals of the laser intensity for the master and slave lasers are detected simultaneously, and the amount of feedback-control signal is calculated from the subtraction of the two detected signals. The feedback is applied to the pumping power of the microchip laser in the slave laser for synchronization. It is found that the synchronization regions obtained by the incoherent feedback method are much smaller than those obtained by the coherent coupling method. Dual synchronization of chaos is also demonstrated by using the coherent coupling scheme for multi-user communication applications. Dual synchronization of chaos is achieved between the corresponding pairs independently under injection locking.

For communication applications, the chaotic masking method with both digital and analog messages has been demonstrated. For the transmission of a digital message, the transmitted binary signals can be determined by knowing the accuracy of chaos synchronization in the receiver. For the transmission of an analog message, the chaotic laser output is externally modulated with a sinusoidal waveform. It is found that message recovery can succeed at a lower modulation frequency than the relaxation oscillation frequency.

Finally, a new scheme for the generation of information-theoretic secure keys has been introduced, whose security can be guaranteed quantitatively by probability theory and by the fact that an adversary's information is limited. It has been experimentally shown that the probability of an eavesdropper coincidentally acquiring the same samples as the two justified users can be set sufficiently small. This method does not require synchronization between two chaotic lasers and the degree of security can be estimated quantitatively.

Acknowledgements

We acknowledge Peter Davis, Satoko Itaya, Fumihiko Kannari, Satoshi Kinugawa, Yun Liu, Takanori Matsuura, Ryan McAllister, Riccardo Meucci, Takeshi Ogawa, Rajarshi Roy, and Masahiko Shinozuka for their contribution to the studies presented in this article. A. Uchida thanks Peter Davis and Rajarshi Roy for fruitful discussion. A. Uchida acknowledges the support from Japan Society for the Promotion of Science (JSPS) Postdoctoral Fellowships for Research Abroad.

References

[1] J.-P. Goedgebuer, L. Larger, H. Porte, Phys. Rev. Lett. 80 (1998) 2249–2252.
[2] L. Larger, J.-P. Goedgebuer, F. Delorme, Phys. Rev. E 57 (1998) 6618–6624.
[3] G.D. VanWiggeren, R. Roy, Science 279 (1998) 1198–1200.
[4] A.E. Siegman, Lasers, University Science Books, Mill Valley, CA, 1986.
[5] A. Uchida, T. Ogawa, M. Shinozuka, F. Kannari, Phys. Rev. E 62 (2000) 1960–1971.
[6] A. Uchida, M. Shinozuka, T. Ogawa, F. Kannari, Opt. Lett. 24 (1999) 890–892.
[7] C.L. Tang, H. Statz, G. deMars, J. Appl. Phys. 34 (1963) 2289.
[8] P. Mandel, Theoretical Problems in Cavity Nonlinear Optics, Cambridge University Press, Cambridge, UK, 1997.
[9] K. Otsuka, Nonlinear Dynamics in Optical Complex Systems, KTK Scientific, Tokyo, Japan, 1999.
[10] A. Uchida, T. Matsuura, S. Kinugawa, S. Yoshimori, Phys. Rev. E 65 (2002) 066212.
[11] A. Uchida, R. McAllister, R. Meucci, R. Roy, Phys. Rev. Lett. 91 (2003) 174101.
[12] L.S. Tsimring, M.M. Sushchik, Phys. Lett. A 213 (1996) 155–166.
[13] Y. Liu, P. Davis, Phys. Rev. E 61 (2000) R2176–R2179.
[14] A. Uchida, S. Kinugawa, T. Matsuura, S. Yoshimori, Phys. Rev. E 67 (2003) 026220.
[15] A. Uchida, S. Kinugawa, T. Matsuura, S. Yoshimori, Opt. Lett. 28 (2003) 19–21.
[16] J.M. Liu, H.F. Chen, S. Tang, IEEE J. Quantum Electron. 38 (2002) 1184–1196.
[17] S. Sivaprakasam, K.A. Shore, Opt. Lett. 24 (1999) 1200–1202.
[18] I. Fischer, Y. Liu, P. Davis, Phys. Rev. A 62 (2000) 011801(R).

[19] T. Ogawa, A. Uchida, M. Shinozuka, S. Yoshimori, F. Kannari, Japanese J. Appl. Phys. 41 (2002) L1309–L1311.
[20] A. Uchida, Y. Liu, P. Davis, IEEE J. Quantum Electron. 39 (2003) 963–970.
[21] J.-B. Cuenot, L. Larger, J.-P. Goedgebuer, W.T. Rhodes, IEEE J. Quantum Electron. 37 (2001) 849–855.
[22] A. Uchida, S. Yoshimori, M. Shinozuka, T. Ogawa, F. Kannari, Opt. Lett. 26 (2001) 866–868.
[23] A. Uchida, P. Davis, S. Itaya, Appl. Phys. Lett. 83 (2003) 3213–3215.