Synchronization of cascaded chaotic optical rings and secure communications

Kazuyuki Yoshimura

NTT Communication Science Laboratories, NTT Corporation
2-4, Hikaridai, Seika-cho, Soraku-gun, Kyoto, Japan
Phone:+81-774-93-5136, Fax:+81-774-93-5155
Email: kazuyuki@cslab.kecl.ntt.co.jp

1. Introduction

The use of chaos to secure communications has been one of the most appealing applications of chaos. A number of chaos communication methods have been proposed [1], some of which were implemented by using electronic circuits. In addition, much attention has been paid to optical systems [2, 3]. Optical chaos communication was experimentally demonstrated in fiber ring lasers [2] and semiconductor lasers [3]. Conventional data encryption techniques consist of binary operations performed by a conventional digital computer. In contrast, data encryption techniques using optical chaos need no computer and all encryption and decryption procedures can be performed by optical circuits. Therefore, they offer the possibility of high-speed secure data transfer by all-optical systems, i.e., *optical cryptograph*.

Most of the chaos communication schemes so far are, however, unsatisfactory in terms of security level [4]. This is the case also for the optical schemes [5]. Chaos secure communication schemes can be regarded as a kind of secret key cryptoscheme, where parameters in the chaotic systems serve as secret keys. To enhance security it is required that (1) the number of possible key parameter values be large enough to prevent the search by an eavesdropper over all possible key values and (2) the key parameter values be difficult to estimate from the transmitted signal. However, to our knowledge, no optical chaos secure communication system has yet been developed that can satisfy these requirements. In this paper, we propose a full optical model system for secure communications, which consists of cascaded optical rings and includes no electrical feedback. We show that a full optical chaos secure communication system, which can satisfy the above two requirements, is in principle possible.

2. System and Encoding

We study a chaotic optical system consisting of cascaded N optical ring units. Figure 1 illustrates the nth ring unit. ξ_n is an injected electric field from $(n-1)$th to nth unit. Light produced by combining ξ_n and the feedback field passes through a nonlinear medium. For simplicity, we assume it to be a homogeneously broadened two-level absorber. On departing the absorber, the light passes through an optical modulator to acquire phase shift δ_n and then it is amplified by a factor A_n. We use the set $\{\delta_n\}$ of the phase shifts as the secret key parameters. After the amplification, a fraction c_n of the light is fed back to the loop and the other $1-c_n$ fraction is injected into the $(n+1)$th unit. In Fig. 1, $\zeta_n \in \mathbf{C}$ and $w_n \in \mathbf{R}$ represent the complex electric field amplitude at the input point of the absorber and the spatially averaged population inversion, respectively. The difference-differential equations describing this type of optical ring were introduced by Ikeda [6].

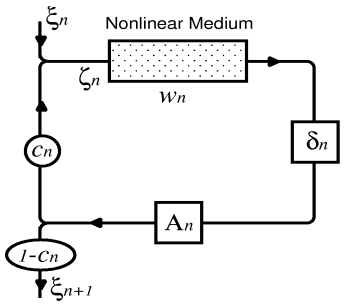

Figure 1: Configuration of optical ring unit.

Figure 2 shows the configuration of the communication system. E_I is a monochromatic injected field with a constant amplitude. U_n $(n = 1, \ldots, N)$ represents the ring unit of the transmitter illustrated in Fig. 1 and U'_n $(n = 1, \ldots, N)$ the unit of the receiver, which is the same as U_n. Those units are coupled by injecting the output field of the nth unit into the $(n+1)$th unit. The output of U_N is separated into two paths, which are assumed to have different lengths, and then those lights are coupled again. We denote the light after the coupling by

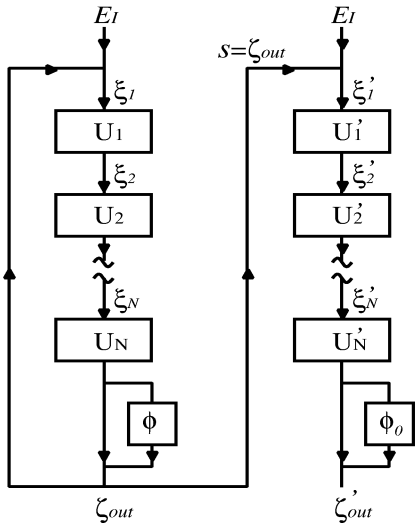

Figure 2: Configuration of communication system.

ζ_{out} and the corresponding light in the receiver by ζ'_{out}. ζ_{out} is fed back and added to E_I to form the input field for U_1. ζ_{out} is also used as the transmitted signal s and the input for U'_1 is given by $s + E_I$.

The light entering one of the branched paths acquires phase shift ϕ, when passing through an optical modulator. This modulator encodes the binary messages by alternating ϕ between two different values at an interval of T: $\phi = \phi_0$ for binary message '0' and $\phi = \phi_1$ for '1'. In the receiver, the corresponding phase shift is fixed to ϕ_0. The output of U'_N is the same as that of U_N when each U'_n synchronizes with the corresponding U_n. Therefore, $\zeta'_{out} = \zeta_{out}$ if $\phi = \phi_0$ while $\zeta'_{out} \neq \zeta_{out}$ if $\phi = \phi_1$. We define the average error between the intensities of s $(= \zeta_{out})$ and ζ'_{out} by $e_m = T^{-1} \int_{(m-1)T}^{mT} |I_s(t) - I'(t)|\, dt$, where $I_s = |s|^2$, $I' = |\zeta'_{out}|^2$, and m is an integer. The mth binary message b can be decoded as $b = 0$ if $e_m < e_c$ otherwise $b = 1$, where e_c is some threshold.

3. Model

The difference-differential equations describing the transmitter system are given as follows:

$$\begin{aligned} &dw_n/dt = f(w_n(t), \zeta_n(t)), \\ &\zeta_n(t) = g_n(w_n(t-\tau_n), \zeta_n(t-\tau_n); \delta_n) + \xi_n(t), \end{aligned} \tag{1}$$

where

$$\begin{aligned} &f(w, \zeta) = -\gamma\{w + 1 + |\zeta|^2(\exp[Gw] - 1)/G\}, \\ &g_n(w, \zeta; \delta_n) = c_n A_n \zeta \exp[(\beta + i\alpha)w + i(\kappa_n + \delta_n)], \end{aligned}$$

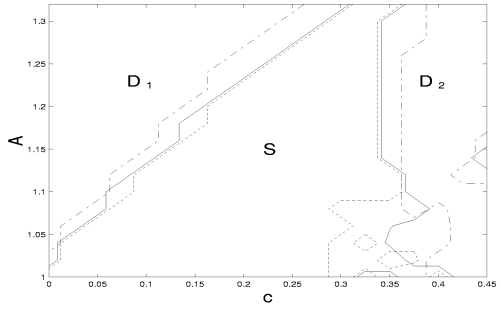

Figure 3: Region of synchronized motion for N=5 (dash-dotted line), 10 (solid line), and 15 (dashed line).

and

$$\xi_n(t) = \begin{cases} \zeta_{out}(t) + E_I e^{i\Delta\omega t}, & n = 1, \\ (1 - c_{n-1}) A_{n-1} \zeta_{n-1}(t - \tau_{n-1}) & \\ \quad \times \exp[(\beta + i\alpha) w_{n-1}(t - \tau_{n-1})] & \\ \quad \times \exp[i(\kappa_{n-1} + \delta_{n-1})], & n = 2, \ldots, N. \end{cases} \tag{2}$$

The output field is given by

$$\begin{aligned} \zeta_{out}(t) &= \frac{1}{2}(1 - c_N) A_N \exp[i(\kappa_N + \delta_N)] \\ &\times \{\zeta_N(t - \tau_{b,0}) \exp[(\beta + i\alpha) w_N(t - \tau_{b,0})] \\ &+ \zeta_N(t - \tau_{b,1}) \exp[(\beta + i\alpha) w_N(t - \tau_{b,1}) + i\phi]\}. \end{aligned} \tag{3}$$

In these equations, β and α are nonlinear gain coefficients, γ is the atomic decay rate, G another gain-related parameter, and κ_n the phase acquired by a plane wave traversing the ring. τ_n is the round trip time of the nth ring. $\tau_{b,0}$ and $\tau_{b,1}$ are the delay times for the two branched paths after U_N.

We denote the receiver's variable by a prime. The equations for the receiver are given by

$$\begin{aligned} &dw'_n/dt = f(w'_n(t), \zeta'_n(t)), \\ &\zeta'_n(t) = g_n(w'_n(t - \tau_n), \zeta'_n(t - \tau_n); \delta_n) + \xi'_n(t), \end{aligned} \tag{4}$$

where ξ'_n $(n = 2, \ldots, N)$ is given by replacing w_{n-1} and ζ_{n-1} with w'_{n-1} and ζ'_{n-1} in Eq. (2), respectively. ξ'_1 is given by $\xi'_1 = s(t) + E_I e^{i\Delta\omega t}$, where $s(t) = \zeta_{out}(t)$. ζ'_{out} is also given by the same replacements in Eq. (3).

4. Synchronization

When $\zeta_n(t) = \zeta'_n(t)$ $(n = 1, \ldots, N)$ the equations (1) and (4) are precisely the same and identical synchronization is thus possible. Although it is difficult to prove that the synchronization of systems (1) and (4) occurs for arbitrary initial conditions, we can prove it in the limit

$\gamma \to \infty$, $G \to 0$, $\Delta\omega = 0$, and $dw_n/dt = 0$. In this limit, Eqs. (1) and (4) reduce to the maps

$$\zeta_n(t) = g_n(-1/(1+|\zeta_n(t-\tau_n)|^2), \zeta_n(t-\tau_n); \delta_n) + \bar{\xi}_n(t), \quad (5)$$

$$\zeta'_n(t) = g_n(-1/(1+|\zeta'_n(t-\tau_n)|^2), \zeta'_n(t-\tau_n); \delta_n) + \bar{\xi}'_n(t), \quad (6)$$

where $\bar{\xi}_n$ is given by replacing w_n with $-1/(1+|\zeta_n|^2)$ and substituting $\Delta\omega = 0$ in Eqs. (2) and (3). $\bar{\xi}'_n$ can be obtained in the same manner using the expression for ξ'_n. We can prove the following proposition, which gives a sufficient condition for synchronization.

Proposition. If $\beta \geq 0$ and $c_n A_n < 1/(|\alpha| + \beta/2 + 1)$ $(n = 1, \ldots, N)$ then systems (5) and (6) synchronize for any initial conditions, i.e., $|\zeta_n(t) - \zeta'_n(t)| \to 0$ $(n = 1, \ldots, N)$ for $t \to \infty$.

This proposition states that for any large number N of the units the cascaded systems can synchronize if the feedback strength $c_n A_n$ of each unit is small enough in the above limit. This strongly suggests that synchronization can occur even in systems (1) and (4) when $c_n A_n$ is small and that N can be made large.

We numerically integrated systems (1) and (4) with different initial conditions to examine whether the systems synchronize using the fourth order Runge-Kutta scheme for the differential equations for w_n and w'_n with a fixed time step $\Delta t = 10^{-3}$. We assumed $c_n = c$, $A_n = A$ $(n = 1, \ldots, N)$ and carried out numerical integrations for various c and A. For a set of c and A, we made calculations for five different initial conditions. We examined three different system sizes $N = 5, 10,$ and 15. The other parameters were set as follows: $E_I = 1, \Delta\omega = 0, \gamma = 2, G = 0.02, \beta = 0.01, \alpha = 12,$ $\kappa_n = 0, \delta_n = 0,$ and $\phi = \phi_0 = 0$. As for the delay times, we assigned different values to τ_n because ζ_n tends to diverge if all of τ_n are the same.

Figure 3 shows the parameter region S where synchronized and bounded motion is observed for all of the five initial conditions. We defined that synchronization occurs if $\sum_{n=1}^{N} |\zeta_n - \zeta'_n|$ becomes small and remains less than 10^{-10} for some duration. D_1 is the region where synchronization occurs but the motion diverges. D_2 is the region for unsynchronized and bounded motion. Figure 3 shows that synchronized and bounded motion is observed over a wide range of (c, A). It should be noted that the synchronous region S does not significantly shrink as N increases. This indicates that synchronization can be achieved for large N.

5. Data transmission

We demonstrate that binary data transmission is possible using systems (1) and (4). We set the parameters as follows: $N = 8, \delta_n = 0, c_1 = c_2 = 0.15, c_n = 0.15 + 0.2(n-3)/3$ $(n = 3, \ldots, 6), c_7 = c_8 = 0.35, A_n = 0.9 + 1.2c_n, \phi_0 = 0, \phi_1 = \pi, T = 1,$ and $e_c = 0.1$. The other parameter values are the same as described before. Figure 4(a) shows an example of intensity $I_s(t)$ of the transmitted signal s. In Fig. 4(b), we show the encoded binary messages (upper) and the recovered binary messages (lower). The messages are correctly recovered except for small t, where synchronization is not achieved.

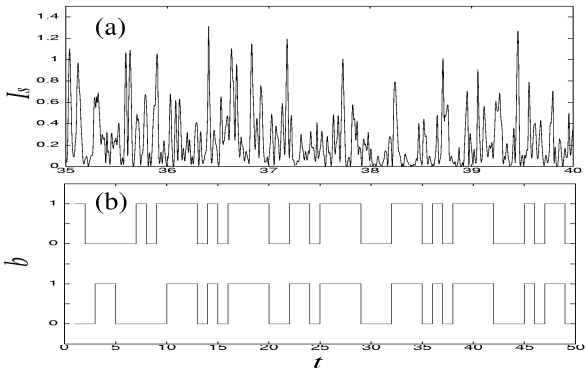

Figure 4: (a) Intensity I_s of transmitted signal. (b) Encoded (upper) and recovered (lower) messages.

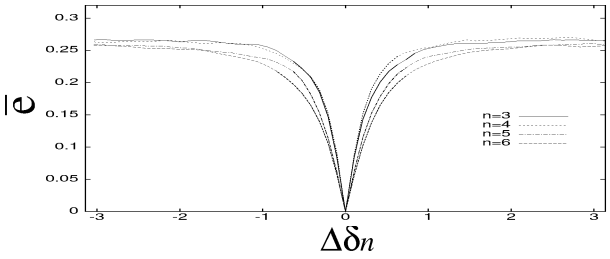

Figure 5: Synchronization error $\bar{e}$ vs. $\Delta\delta_n$.

6. Security

We assume that only the values of set $\{\delta_n\}$ are secret. It should be noted that values of δ_ns can be easily changed in an experimental setup by varying the voltage applied to the optical modulators. Only δ_n $(1 < N_1 \leq n \leq N_2 < N)$ is used as the key because we found that δ_n for small n or large n is not suitable for the key.

It is important to know how the synchronization is sensitive to difference $\Delta\delta_n$ in δ_n between the transmitter and the receiver when $\phi = \phi_0$. In Fig. 5, the average synchronization error defined by $\bar{e} = T_0^{-1} \int_0^{T_0} |I_s(t) - I'(t)|\, dt$, where $T_0 = 500$, is plotted

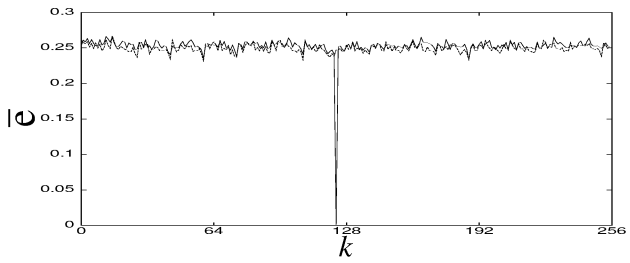

Figure 6: Synchronization error $\bar{e}$ vs. receiver's k for $\phi = \phi_0$ (solid line) and $\phi = \phi_1$ (dashed line).

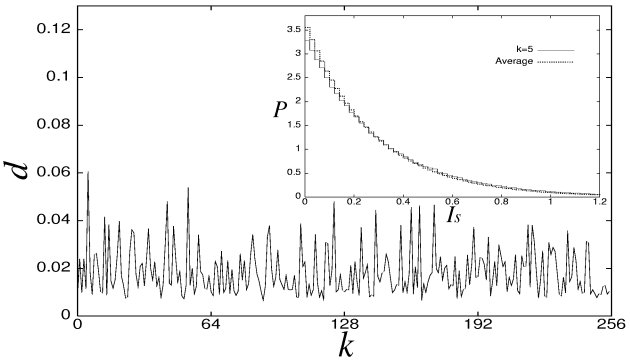

Figure 7: Deviation $d(k)$ vs. k

against $\Delta\delta_n$ ($N_1 = 3 \leq n \leq N_2 = 6$). We set $\delta_n = 0$ in the transmitter and introduced the difference to one of the δ_ns in the receiver. The other parameter values are the same as used in the experiment shown in Fig. 4. It can be seen that $\bar{e}$ increases gradually as $|\Delta\delta_n|$ increases, implying that the recovery of messages is still possible under small mismatches in δ_ns.

In Fig. 5, we can see that $\bar{e}$ fully develops for $|\Delta\delta_n| \geq \pi/2$. This implies that the recovery of the messages is impossible when $|\Delta\delta_n| \geq \pi/2$. Therefore, we assume that each δ_n takes four discrete values $\delta_n \in \{0, \pi/2, \pi, 3\pi/2\}$ and thus one δ_n serves as a secret key for two bits. The number of total possible key values is given by $2^{2(N_2-N_1+1)}$. This number increases rapidly and becomes a huge number as N increases. Therefore, it is impossible to search over all of the possible key values when N is large, e.g., when N is of the order of a few tens. We can define a one-to-one correspondence between an integer k and $\{\delta_n\}$ by $k = \sum_{n=N_1}^{N_2} 2^{2(n-N_1)}\delta_n/(\pi/2)$. In Fig. 6, we show $\bar{e}$ averaged over $T_0 = 500$ as a function of the key number k used in the receiver for two cases of $\phi = \phi_0$ and $\phi = \phi_1$. The key used in the transmitter is fixed as $k = 123$. Significant difference in $\bar{e}$ between $\phi = \phi_0$ and $\phi = \phi_1$ is observed only for $k = 123$. This shows that message recovery by measuring the synchronization error is possible only if the keys are identical between the transmitter and the receiver.

To enhance security, the key should be difficult to estimate from the statistics of the transmitted signal $s(t)$. Let $P(I_s; k, \phi)$ ($\int_0^\infty P(I; k, \phi)dI = 1$) be the probability distribution of I_s for key k and $P_{\rm av}$ the probability distribution averaged over all possible k, where ϕ represents the phase modulation for encoding. We define the deviation of $P(I_s; k, \phi_0)$ from $P_{\rm av}(I_s; \phi_0)$ by $d(k) = \int_0^\infty |P(I; k, \phi_0) - P_{\rm av}(I; \phi_0)|dI$. Figure 7 shows $d(k)$ plotted against k. In the inset, we show $P_{\rm av}(I_s; \phi_0)$ (dashed line) and $P(I_s; k, \phi_0)$ (solid line) for $k = 5$ that gives the largest $d(k)$. We can see that $d(k)$ is very small for all k and there is no significant dependence of $P(I_s; k, \phi_0)$ on k. It is practically difficult to distinguish $P(I_s; k, \phi_0)$s corresponding to different ks. This implies that at least the measurement of the probability distribution of I_s gives no information about the key to an eavesdropper. In this sense, the set $\{\delta_n\}$ of the phase shifts is suitable for use as keys.

7. Summary

We have demonstrated the synchronization of cascaded optical rings and shown that by using this technique there exists the possibility of a full optical chaos secure communication system, which can satisfy the basic requirements on secret keys. We have also shown that the set of the phase shifts can be used as good secret keys.

References

[1] K. M. Cuomo and A. V. Oppenheim, Phys. Rev. Lett. **71**, 65 (1993); L. Kocarev and U. Parlitz, Phys. Rev. Lett. **74**, 5028 (1995); K. Yoshimura, Phys. Rev. E **60**, 1648 (1999).

[2] G. D. VanWiggeren and R. Roy, Phys. Rev. Lett. **81**, 3547 (1998).

[3] J. P. Goedgebuer, L. Larger, and H. Porte, Phys. Rev. Lett. **80**, 2249 (1998); I. Fischer, Y. Liu, and P. Davis, Phys. Rev. A **62**, 011801(R) (2000).

[4] K. M. Short, Int. J. Bifurcation and Chaos **4**, 957 (1994); G. Pérez and H. A. Cerdeira, Phys. Rev. Lett. **74**, 1970 (1995).

[5] J. B. Geddes, K. M. Short, and K. Black, Phys. Rev. Lett. **83**, 5389 (1999).

[6] K. Ikeda, Optics Commun. **30**, 257 (1979).