High-speed chaotic communication using an optical fibre ring as a key*

Zou Lin(邹 琳), Feng Ye(冯 野), Yang Yi-Biao(杨毅彪)†,
Wang An-Bang(王安帮), Yang Ling-Zhen(杨玲珍), and Zhang Jian-Zhong(张建忠)

Institute of Optoelectronic Engineering, Department of Physics & Optoelectronics, Taiyuan University of Technology, Taiyuan 030024, China

(Received 16 December 2010; revised manuscript received 27 January 2011)

A chaotic communication scheme with a fibre ring inserted in the optical feedback of the transmitter laser as an additional key is proposed under anticipating synchronization. The numerical results show that the key can enhance the communication security effectively. It is theoretically safe for the communication scheme to transmit messages with a frequency beyond the relaxation oscillation frequency.

Keywords: chaotic communication, optical fibre ring, semiconductor lasers

PACS: 42.65.Sf, 05.45.Vx **DOI:** 10.1088/1674-1056/20/9/094209

1. Introduction

With the development of communication networks, information security becomes more and more important. Many researchers have devoted themselves to chaotic laser communication and have proposed many communication schemes based on the fibre laser[1] and the semiconductor laser[2−8] to implement the high-speed physical-layer security technique. The most enthusiastically studied schemes are based on the semiconductor laser, which is an ideal source apparatus for traditional communication due to its inherent advantages. It presents chaotic oscillation only under external perturbations such as optoelectronic feedback,[4] electro-optic (EO) feedback[5] and all-optical external cavity feedback.[6]

In chaotic communication, a message is commonly modulated by using the chaotic waveform, which is realized through chaotic masking (CMS)[9] and chaotic shift keying (CSK).[10] On the receiver side, the laser with the chaotic carrier being injected into it achieves generalized synchronization through injection locking. Affected by the filtering characteristic, the receiver laser outputs the same chaotic carrier without the message. Then the message is decoded by subtracting the output of the receiver laser from the total transmitted signal. In the traditional scheme, to make the communication safe, the transmitter is always trying to prevent an eavesdropper laser from achieving synchronism with it. Nevertheless, a generalized synchronization system has a great tolerance for internal parameter mismatches.[10] What is more, it is possible to estimate the parameters (such as the pumping parameter and the feedback gain) and the external cavity length of chaotic lasers by the analysing time series,[11,12] which means that it is not difficult for an eavesdropper to make its laser achieve the synchronization with that of the transmitter through injection locking. In addition, a single laser diode can achieve generalized synchronization though an open-loop configuration[10,13] or through a bandwidth-enhanced system that has a more complex structure.[14] It predicts that a more complex system cannot prevent an eavesdropper from achieving generalized synchronization with the transmitter. So the only way to improve security is to find a new communication method, which makes it impossible to decode the message by using the filtering characteristic.

The filtering characteristic is very weak when the message frequency is not lower than the relaxation oscillation frequency.[15] The additional chaos modulation (ACM), in which the filtering characteristic is not used to decode the message, is a very effective method

*Project supported by the Key Program of National Natural Science Foundation of China (Grant No. 60927007), the National Natural Science Foundation of China (Grant No. 60908014), and the Shanxi Provincial Science Foundation for Youths, China (Grant No. 2010021003-4).

†Corresponding author. E-mail: yangyibiao_tyut@sohu.com

© 2011 Chinese Physical Society and IOP Publishing Ltd

to transmit a high frequency message beyond the relaxation frequency.[16,17] It creates the possibility to prevent eavesdroppers from cracking the message with the filtering characteristic. In this method, a message is encoded by adding it to the chaotic waveform, it is sent equally to both the transmitter and the receiver, and then decoded by subtracting the output of the receiver laser from the transmission signal, which is different from CSK and CMS.

The anticipating synchronization, which has already been experimentally demonstrated in previous work,[18,19] is stable and robust.[20] It allows the GHz-frequency detuning, so the schemes based on it could be very practical.

In this paper, we propose a chaotic communication scheme with a fibre ring inserted in the optical feedback of the transmitter laser as an additional key. The ability to transmit the message beyond the relaxation oscillation frequency is proved first. Then a fibre ring is inserted into the external cavity as the key. Finally we prove that it is difficult for eavesdroppers to obtain the message transmitted beyond the relaxation oscillation frequency by using the filtering characteristic.

2. Schematic setup

A functional block diagram of the system is depicted in Fig. 1. The output light from the transmitter laser (TL) is divided into two beams. One is coupled back to the TL itself through an optical circulator (OC) and the other is injected by the receiver into its laser (RL) via another OC. Under the anticipating synchronization, the message is encoded by adding it to the chaotic output of the TL and decoded by subtracting the chaotic carrier from the output of the RL.

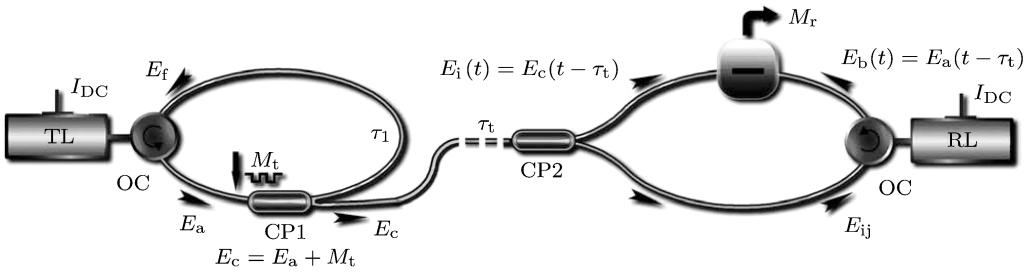


Fig. 1. Open-loop chaotic communication schematic under anticipating synchronization. CP1 and CP2 are couplers, I_{DC} is the pump current.

The dynamics of the slowly varying laser field E, the phase Φ and the carrier density N are governed by[21]

$$\frac{\mathrm{d}E_{a,b}(t)}{\mathrm{d}t} = \frac{1}{2}\left(\Gamma G_{a,b} - \frac{1}{\tau_p}\right)E_{a,b}(t) + k_{a,b}M_{f,ij}(t)\cos\theta_{a,b}(t), \quad (1)$$

$$\frac{\mathrm{d}\Phi_{a,b}(t)}{\mathrm{d}t} = \frac{1}{2}\alpha\left(\Gamma G_{a,b} - \frac{1}{\tau_p}\right) - k_{a,b}\frac{M_{f,ij}(t)}{E_{a,b}(t)}\sin\theta_{a,b}(t), \quad (2)$$

$$\frac{\mathrm{d}N_{a,b}(t)}{\mathrm{d}t} = \frac{I}{qV} - \frac{1}{\tau_N}N_{a,b}(t) - G_{a,b}\left|E_{a,b}(t)\right|^2, \quad (3)$$

$$G_{a,b}(t) = G[N_{a,b}(t) - N_0]/[1 + \varepsilon\left|E_{a,b}(t)\right|^2], \quad (4)$$

$$M_f(t)\exp[\mathrm{i}\Phi_f(t)] = E_a(t-\tau_1)\exp[-\mathrm{i}\omega_a\tau_1 + \mathrm{i}\Phi(t-\tau_1)], \quad (5)$$

$$M_{ij}(t)\exp[\mathrm{i}\Phi_{ij}(t)] = E_a(t-\tau_{ij})\exp[-\mathrm{i}\omega_a\tau_{ij} + \mathrm{i}\Phi(t-\tau_{ij}) - \mathrm{i}\Delta\omega(t-\tau_{ij})], \quad (6)$$

$$\theta_a(t) = \Phi_a(t) - \Phi_f(t) = \omega_a\tau_1 + \Phi_a(t) - \Phi_a(t-\tau_1), \quad (7)$$

$$\theta_b(t) = \Phi_b(t) - \Phi_{ij}(t) + t\Delta\omega = \omega_a\tau_{ij} + \Phi_b(t) - \Phi_a(t-\tau_{ij}) + t\Delta\omega, \quad (8)$$

where subscripts a and b denote TL and RL, respectively, I represents the pump current, ω_a is the transmitter laser frequency at the solitary oscillation and $\Delta\omega = \omega_a - \omega_b$ denotes the angular frequency detune between the two lasers. The $\tau_1 = 0.2$ ns is the feedback delay and $\tau_{ij} = 1.2$ ns is the delay time of the injected light. The k_a is the feedback coefficient of the external cavity lasers, k_b is the optical injection coefficient. They are defined as:

$$k_{a,b} = \frac{1}{\tau_{in}}\frac{(1-r_0)^2 r_{a,b}}{r_0}, \quad (9)$$

where r_a and r_b represent the percentages of the TL feedback and the RL injection, respectively. The other parameters used in the simulation are listed in Table 1.

Table 1. Parameters used in the numerical simulation.

Symbol	Parameter	Value
V	volume of the active region	1.5×10^{-16} m^3
Γ	optical confinement factor	0.4
$\tau_{\rm n}$	carrier lifetime	2 ns
$\tau_{\rm p}$	photon lifetime	2 ps
$\tau_{\rm in}$	round-trip time in internal laser cavity	10 ps
r_0	reflection rate of the laser facet	30%
$N_{\rm th}$	carrier density at threshold	2×10^{24} m^{-3}
N_0	carrier density at transparency	10^{24} m^{-3}
G	gain coefficient	2.1×10^{-12} m^3/s
α	linewidth enhancement factor	5.5
$I_{\rm th}$	threshold current	12.5 mA
λ	wavelength	1550 nm
q	charge quantity	1.6×10^{-19} C

The message recovery performance is examined by calculating the signal-to-noise ratio (SNR). Detuning $\Delta\nu$ ($= \Delta\omega/2\pi$) is set to be -11 GHz and -14 GHz, respectively,[20] pump current $I = 1.7I_{\rm th}$. The signal amplitude is about 7% of the amplitude of the chaotic waveform. A high SNR, which is nearly independent of the message frequency, can be obtained using the anticipating synchronization, as shown in Fig. 2(a). There is some fluctuation in each curve, which may be caused by the randomness of the chaotic carrier. The GHz detuning influences the synchronism and communication performance slightly under the anticipating synchronization, which is different from that under the complete synchronization.[22,23]

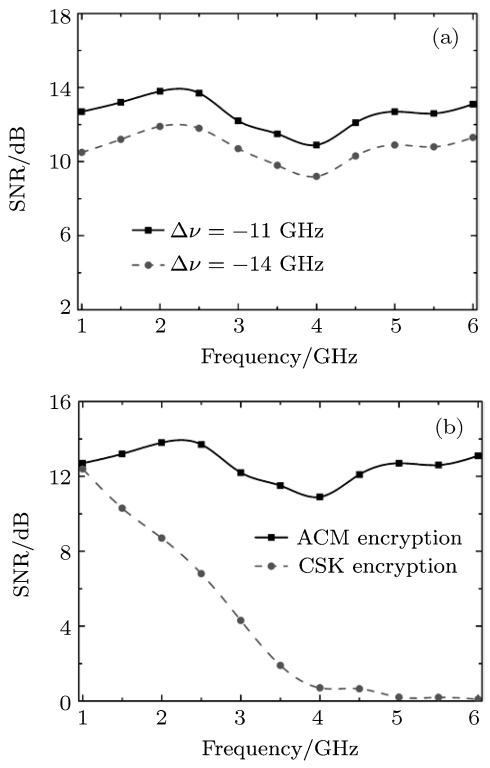


Fig. 2. SNR versus message frequency: (a) for the anticipating synchronization: $r_{\rm a} = 0.27$, $r_{\rm b} = 0.45$, (b) for different encryption schemes.

To prove the advantage of ACM on transmitting the high frequency message, the SNRs of CSK and ACM under different transmission frequencies are presented in Fig. 2(b). The SNR shows no connection with the message frequency in the case of using ACM, whereas the SNR declines as the message frequency increases while using CSK. In addition, the SNR of the message decreases to below 2 dB when the message frequency increases to the relaxation frequency (3.8 GHz). The communication quality is poor in this situation. The performance of ACM is acceptable at higher bit rates. This result agrees with the conclusion of Ref. [17].

3. Improving security through a fibre ring and high speed

To make the scheme theoretically safe, two necessary conditions are needed, i.e., the system has a security key and the injection locking is useless for cracking the message.

3.1. Importing a fibre ring as the key

It is necessary to import a key to enhance security due to the principles of ACM. In a conventional ACM encryption method, the chaotic carrier is sent equally to both the TL and the RL, and the RL turns into synchronism with the TL by injecting the receiving

chaotic carrier. Hence, an eavesdropper might intercept the chaotic carrier, synchronize with the TL and crack the message.

As shown in Fig. 3, we insert a fibre ring (component J) into the external cavity, which is plotted in shadow. It is an additional key, which does not influence the transmission speed. The $M_{\mathrm{f,ij}}$ and $\Phi_{\mathrm{f,ij}}$ can be described by the following equations,

$$\begin{aligned} & M_{\mathrm{f}}(t)\exp[\mathrm{i}\Phi_{\mathrm{f}}(t)] \\ = & \sqrt{1-\rho}E_{\mathrm{a}}(t-\tau_{\mathrm{f}})\exp\{\mathrm{i}[-\omega_{\mathrm{a}}\tau_{\mathrm{f}}+\Phi(t-\tau_{\mathrm{f}})]\} \\ & +\mathrm{i}\sqrt{\rho}E_{\mathrm{p}}(t-\tau_2)\exp\{\mathrm{i}[\varphi_{\mathrm{p}}(t-\tau_2)-\omega_{\mathrm{a}}\tau_2]\}, \quad (10) \\ & M_{\mathrm{ij}}(t)\exp[\mathrm{i}\Phi_{\mathrm{ij}}(t)] \\ = & \sqrt{1-\rho}E_{\mathrm{a}}(t-\tau_{\mathrm{ij}})\exp\{\mathrm{i}[-\omega_{\mathrm{a}}\tau_{\mathrm{ij}}+\mathrm{i}\Phi(t-\tau_{\mathrm{ij}}) \\ & +\Delta\omega(t-\tau_{\mathrm{ij}})]\}+\mathrm{i}\sqrt{\rho}E_{\mathrm{p}}(t-\tau_2) \\ & \times\exp\{\mathrm{i}[\varphi_{\mathrm{p}}(t-\tau_2)-\omega_{\mathrm{a}}\tau_2+\Delta\omega(t-\tau_{\mathrm{ij}})]\}, \quad (11) \\ & E_{\mathrm{p}}(t)\exp[\mathrm{i}\varphi_{\mathrm{p}}(t)] \\ = & \mathrm{i}\sqrt{1-\rho}E_{\mathrm{a}}(t-\tau_{\mathrm{f,ij}})\exp\{\mathrm{i}[\Phi(t-\tau_1)-\omega_{\mathrm{a}}\tau_{\mathrm{k,ij}}]\} \\ & +\sqrt{\rho}E_{\mathrm{p}}(t-\tau_2)\exp\{\mathrm{i}[\varphi_{\mathrm{p}}(t-\tau_2)-\omega_{\mathrm{a}}\tau_2]\}, \quad (12) \end{aligned}$$

where φ_{p} denotes the phase term; ρ represents the coupling coefficient; $E_{\mathrm{p}}(t)$ is the circulated component; τ_1 and τ_2 refer to the delay time of the external cavity and the fibre ring, respectively; τ_2 can be described as $\tau_2 = ln/c = 1.5l/c$, with $l = 0.6$ m being the length of the fibre ring and n the fibre refractive index.

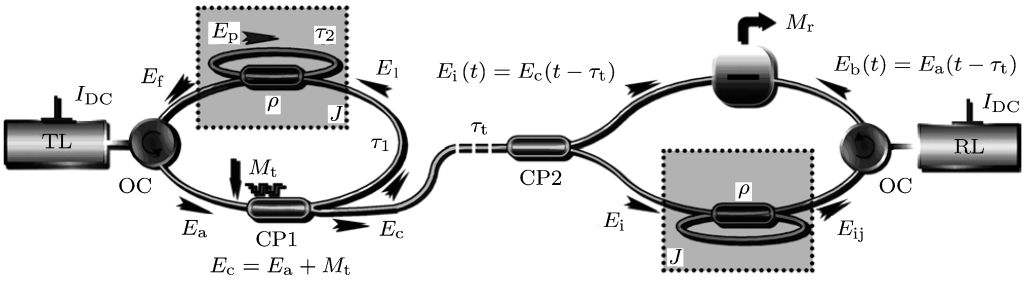


Fig. 3. Schematic diagram of chaotic optical communication using a fibre ring as an additional key.

The influence of the fibre ring on security is examined when no laser intrinsic parameter mismatch is considered. The coefficient ρ of the fibre ring is assumed to be 0.1. In the simulation, a 2.25 Gbps random bit sequence modulated by a 4.5 GHz sinusoidal subcarrier is hidden into the chaotic carrier and transmitted to the receiver, as shown in Fig. 4. The decoding performances under different situations are displayed in Figs. 5(a), 5(b) and 5(c). The TL and the RL without or with the fibre ring simultaneously can ensure the high quality message decoding, as displayed in Figs. 5(a) and 5(c). However, when only the TL has a fibre ring, the extraction of messages fails, as shown in Fig. 5(b). These results indicate that the fibre ring can be used as an additional key for enhancing security. In addition, the influence of the fibre ring length mismatch on the extracted message quality is analysed and is shown in Fig. 6. It can be discovered that the SNR is extremely sensitive to the mismatch of the fibre ring length. A small deviation in the fibre ring length can prevent the eavesdropper from cracking the message.

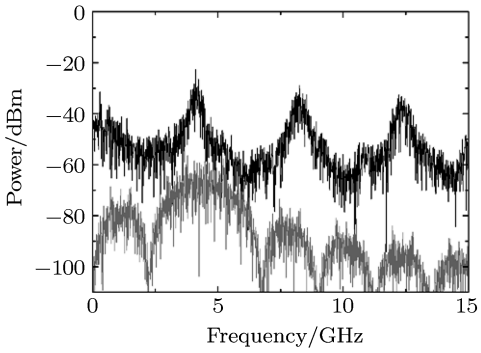


Fig. 4. Power spectra of a 2.25 GHz random message with (black) and without (gray) chaotic encryption.

The effect of the insertion of the fibre ring is to make the transmitter feedback (E_{f}) different from that of the chaotic carrier (E_{c}). That is because when an eavesdropper intercepts E_{c}, he can estimate the internal parameter by analysing the time series,[11] if E_{f} and E_{c} are the same, he may synchronize with the transmitter without utilizing injection locking, as there is little difference between an eavesdropper and a legal receiver.

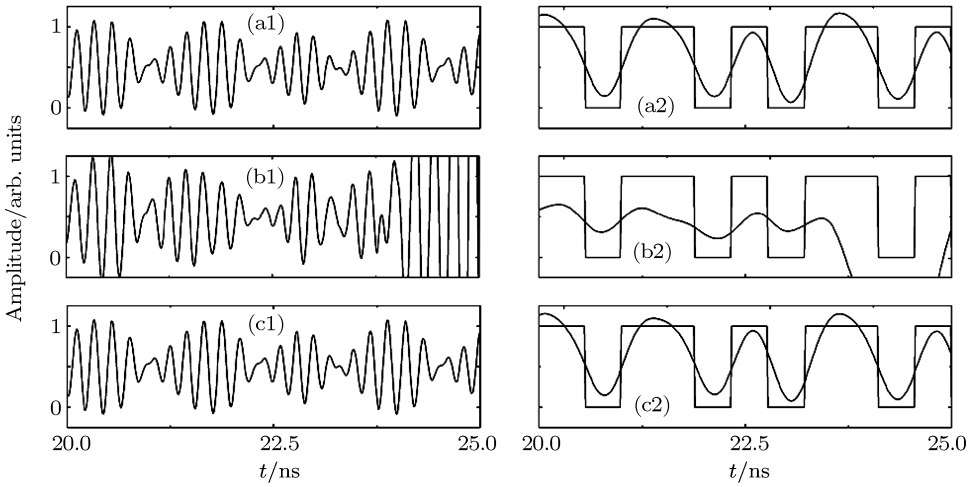


Fig. 5. Decoding message performance for: (a) transmitter and receiver without fibre ring; (b) transmitter with fibre ring, while receiver without fibre ring; (c) transmitter and receiver with fibre ring.

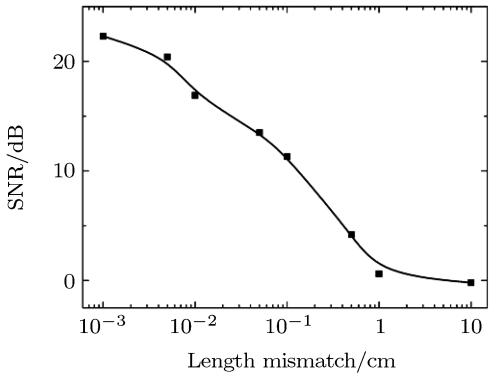


Fig. 6. SNR as a function of fibre ring length mismatch.

3.2. Transmission frequency selection

In Ref. [10], it has been shown that the receiver can achieve generalized synchronization with an open-loop structure and decode the message by using the filtering characteristic. Thus, it is also possible for an eavesdropper to crack the message with an open-loop structure and ignore the external cavity including the fibre ring. In this section, instead of trying to guess the key, the eavesdropper tries to achieve generalized synchronization with an open-loop structure and decode the message by using the filtering characteristic. It is shown that although the eavesdropper can achieve generalized synchronization, it cannot decode the message modulated beyond the relaxation oscillation frequency.

The dynamics of the eavesdropper's semiconductor laser is described by the rate equations,[10]

$$\frac{\mathrm{d}E_\mathrm{e}(t)}{\mathrm{d}t} = \frac{1}{2}\left(\Gamma G_\mathrm{e} - \frac{1}{\tau_\mathrm{p}}\right)E_\mathrm{e}(t) + k_\mathrm{inj}E_\mathrm{a}(t-\tau_\mathrm{inj})\cos\theta_\mathrm{e}(t), \quad (13)$$

$$\frac{\mathrm{d}\Phi_\mathrm{e}(t)}{\mathrm{d}t} = \frac{1}{2}\alpha\left(\Gamma G_\mathrm{e} - \frac{1}{\tau_\mathrm{p}}\right) - k_\mathrm{inj}\frac{E_\mathrm{a}(t-\tau_\mathrm{inj})}{E_\mathrm{e}(t)}\sin\theta_\mathrm{e}(t), \quad (14)$$

$$\frac{\mathrm{d}N_\mathrm{e}(t)}{\mathrm{d}t} = \frac{I}{qV} - \frac{1}{\tau_\mathrm{n}}N_\mathrm{e}(t) - G_\mathrm{e}\left|E_\mathrm{e}(t)\right|^2, \quad (15)$$

$$G_\mathrm{e}(t) = G[N_\mathrm{e}(t) - N_0]/(1+\varepsilon\left|E_\mathrm{e}(t)\right|^2), \quad (16)$$

$$\theta_\mathrm{e}(t) = \omega_\mathrm{a}\tau_\mathrm{inj} + \Phi_\mathrm{e}(t) - \Phi_\mathrm{a}(t-\tau_\mathrm{inj}) + t\Delta\omega, \quad (17)$$

where k_inj represents the eavesdropper injection coefficient, and is defined by

$$k_\mathrm{inj} = \frac{1}{\tau_\mathrm{in}}\frac{(1-r_0)^2 r_\mathrm{inj}}{r_0}, \quad (18)$$

where the injection rate r_inj represents the percentage of the transmitter laser output electrical field amplitude injected into the eavesdropper laser cavity; $r_\mathrm{inj} = 0.6$; $\tau_\mathrm{inj} = \tau_\mathrm{ij}$. Detune $\Delta\nu = \Delta\omega/2\pi = (\omega_\mathrm{a} - \omega_\mathrm{e})/2\pi = 10$ GHz.

The decoding performance of the eavesdropper is examined. In our numerical simulation, the semiconductor laser of the eavesdropper is the same as that of the TL. In the whole process, high quality generalized synchronization is guaranteed through injection locking. Figure 7 shows the message extraction performance of the eavesdropper. The SNR of the cracked message declines rapidly with the message frequency (subcarrier frequency) increasing. Although the laser of the eavesdropper synchronizes with that of the TL, the eavesdropper cannot filter the high frequency message out. The legal receiver can still decode the high frequency message with a high SNR. Thus the message transmission method described in this paper will

be theoretically safe if the frequency of the subcarrier is not lower than the relaxation frequency.

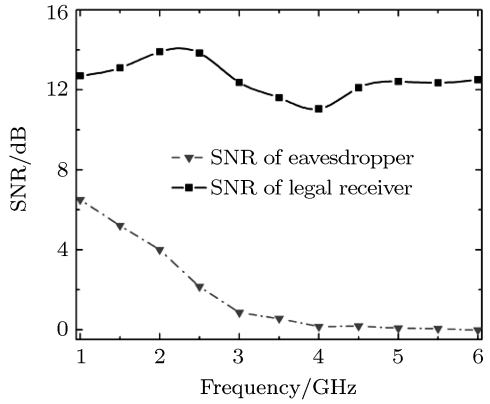


Fig. 7. Decoding performance of the receiver and the eavesdropper, i.e., SNR versus message frequency.

The chaotic waveform cancellation performance is limited by the filtering characteristic when a receiver (legal or illegal) uses generalized synchronization to extract the message. After generalized synchronization is achieved through injection locking, the crucial step to crack the message is to use the filtering characteristic to reproduce the chaotic carrier without the message ($E_{\rm a}$, in Fig. 3). However, this method only works effectively when the message frequency is lower than the relaxation oscillation frequency of the semiconductor laser.[15] Even if the eavesdropper can achieve synchronization through injection locking, only the message below the relaxation frequency may be obtained.

In our scheme, the key that prevents the message from being eavesdropped through injection locking is to transmit the message with a frequency that is not lower than the relaxation oscillation frequency.

4. Conclusion

In this paper, a chaotic communication scheme is proposed with a fibre ring inserted in the external cavity of the transmitter laser as an additional key. The results indicate that the key can enhance the communication security effectively. When this scheme is used to transmit a high frequency message beyond the relaxation frequency, it can be proved theoretically that the scheme is safe. It is noted that there is scope for more detailed study of utilizing vertical cavity surface-emitting lasers or electro-optical systems in this method.

References

[1] van Wiggeren G D and Roy R 1998 *Science* **279** 1198
[2] Mirasso C R, Mulet J and Masoller C 2002 *IEEE Photon. Tech. Lett.* **14** 456
[3] Mirasso C R, Colet P and Garcia-Fernandez P 1996 *IEEE Photon. Technol. Lett.* **8** 299
[4] Goedgebuer J P, Larger L and Porte H 1998 *Phys. Rev. Lett.* **80** 2249
[5] Goedgebuer J P, Levy P, Larger L, Chen C C and Rhodes W T 2002 *IEEE J. Quantum Electron.* **38** 1178
[6] Argyris A, Syvridis D, Larger L, Annovazzi-Lodi V, Colet P, Fischer I, Garcia-Ojalvo J, Mirasso C R, Pesquera L and Shore K A 2005 *Nature* **438** 343
[7] Li G H, Wang A B, Feng Y and Wang Y 2010 *Chin. Phys.* B **19** 070515
[8] Wu D and Li J J 2010 *Chin. Phys.* B **19** 120505
[9] Sivaprakasam S and Shore K A 1999 *Opt. Lett.* **24** 1200
[10] Li X, Pan W, Luo B and Ma D 2006 *IEEE J. Quantum Electron.* **42** 953
[11] Ponomarenkoa V I, Prokhorova M D and Koryukin I V 2005 *Tech. Phys. Lett.* **31** 939
[12] Zhao Q, Wang Y and Wang A 2009 *Appl. Opt.* **48** 3515
[13] Vicente R, Pérez T and Mirasso C R 2002 *IEEE J. Quantum Electron.* **38** 1197
[14] Someya H, Oowada I, Okumura H, Kida T and Uchida A 2009 *Opt. Express* **17** 19536
[15] Li Y, Wang Y and Wang A 2008 *Opt. Commun.* **281** 2656
[16] Liu Y, Chen H F, Liu J M, Davis P and Aida T 2001 *IEEE Trans. Circuits Syst.* I **48** 1460
[17] Liu J M, Chen H F and Tang S 2002 *IEEE J. Quantum Electron.* **38** 1184
[18] Sivaprakasam S, Shahverdiev E M, Spencer P S and Shore K A 2001 *Phys. Rev. Lett.* **87** 154101
[19] Sivaprakasam S, Spencer P S, Rees P and Shore K A 2002 *Opt. Lett.* **27** 1250
[20] Kusumoto K and Ohtsubo J 2003 *IEEE J. Quantum Electron.* **39** 1531
[21] Kanakidis D, Bogris A, Argyris A and Syvridis D 2004 *J. Lightwave Technol.* **22** 2256
[22] Murakami A and Ohtsubo J 2002 *Phys. Rev.* A **65** 033826
[23] Liu Y, Takiguchi Y, Davis P, Aida T and Saito S 2002 *Appl. Phys. Lett.* **80** 4306