

# Security-enhanced chaotic communications with optical temporal encryption based on phase modulation and phase-to-intensity conversion

Jiang, Ning; Zhao, Anke; Wang, Yajun; Liu, Shiqin; Tang, Jianming; Qiu, Kun

**OSA Continuum**

*DOI:*
10.1364/OSAC.2.003422

Published: 15/12/2019

Peer reviewed version

# Security-enhanced chaotic communications with optical temporal encryption based on phase modulation and phase-to-intensity conversion

NING JIANG,[1,2,*] ANKE ZHAO,[1] YAJUN WANG,[1] SHIQIN LIU,[1] JIANMING TANG,[2] AND KUN QIU[1]

[1]*School of Information and Communication Engineering, University of Electronic Science and Technology of China, 2006 Xiyuan Avenue, Chengdu 611731, China*
[2]*School of Electronic Engineering, Bangor University, Dean Street LL57 1UT, Bangor, UK*
**uestc_nj@uestc.edu.cn*

**Abstract:** We propose and numerically demonstrate a security-enhanced chaotic communication system by introducing optical temporal encryption (OTE) into the modulated chaotic carrier (chaos + message). In the proposed scheme, the message is firstly embedded into the original chaotic carrier generated by a conventional external-cavity semiconductor laser (ECSL), and before being transmitted to the receiver end, the modulated chaotic carrier propagates through an OTE module that consists of one phase modulator driven by a secret sinusoidal signal and one dispersive component. Our numerical results indicate that, as a direct result of the spectral expansion effect of the sinusoidal phase modulation and the phase-to-intensity conversion effect of the dispersive component, the original chaotic carrier can be encrypted as an uncorrelated chaotic signal with a flat spectrum and an efficiently-suppressed time delay signature, this greatly enhances the privacy of the modulated chaotic carrier. Moreover, comparing with the conventional ECSL-based chaotic communication systems without OTE, the proposed scheme not only shows significantly higher security against attacks including direct linear filtering and synchronization utilization, but also provide additional physical key space to further enhance the system security. In addition, by making use of the transmission dispersion for decryption, the proposed encryption scheme supports dispersion-compensation-free secure fiber communication, and it also supports centralized encryption/decryption in wavelength division multiplexing secure chaotic communication systems. The proposed scheme provides a novel plug-and-play encryption method for implementation in high-security chaotic communication systems.



## 1. Introduction

Chaos communication has attracted extensive attention for its advantage of physical-layer security enhancement, since Pecora and Carrols demonstrated chaos synchronizations in two chaotic systems [1-3]. Over the last decade, external cavity semiconductor laser (ECSL) has been considered as one of the most promising candidates for all-optical chaotic communications, random bit generation and secure key distribution, since it is easy to obtain wideband chaotic signals from ECSLs with proper feedbacks [4-9]. The experimental demonstrations of all-optical chaotic communications in Athens have proved its feasibility of utilizing ECSLs in commercial optical networks [10]. In conventional ECSL-based chaotic communication systems, after having embedded messages into chaotic carriers, the modulated chaotic carriers (chaos + message) are directly transmitted to the receiver end for message recovery [2-4, 11, 12]. As such, the eavesdropper can easily access the modulated chaotic

carrier from public links. It has been proved that when the bit rate is relatively low, the message hidden in the chaotic carrier can be intercepted by using a linear filter with a proper cutoff frequency, this is termed the direct linear filtering (DLF) attack [13, 14]. In addition, the eavesdropper may also intercept the message by amplifying the chaotic carrier split from the public link and then injecting it into a semiconductor laser to construct a similar chaotic communication system, in virtue of the injection-locking mechanism. This type of attack is referred to as the synchronization utilization attack [13]. Therefore, it is important to further enhance the privacy of the modulated chaotic carrier propagating over a public link, in order to protect the security of the message.

On the other hand, the privacy of a chaotic carrier source is also a crucial issue as it may threat the system security. In the conventional ECSL system, the feedback light is a linear time-delayed replica of the output of a SL, the time delay signature (TDS) that denotes the feedback delay can be easily identified by calculating the autocorrelation, delayed mutual information, or permutation entropy of the chaos waveform [15-18]. Once the eavesdropper knows the precise feedback delay by these TDS identification methods, the eavesdropper can reconstruct an illegal receiver with a similar ECSL with a feedback delay equal to the TDS. Subsequently, the eavesdropper can intercept the message by synchronization utilization attack, i.e., the chaotic carrier split from the public link is firstly amplified and then injected into the illegal receiver ECSL. With the injection-locking effect, the output of the illegal receiver ECSL can synchronize with the link chaotic carrier, and consequently, the message may be intercepted illegally. For this reason, the TDS compression for chaotic carriers is also vital for enhancing the information security of chaotic communication systems.

In this paper, a security-enhanced all-optical chaotic communication system is proposed, where an optical temporal encryption (OTE) making use of phase modulation and phase-to-intensity conversion is introduced to encrypt the modulated chaotic carrier as an uncorrelated wideband and TDS-suppressed chaotic signal prior to its transmission over a public link. At the receiver end, the modulated chaotic carrier is firstly decrypted from the transmitted signal by applying a matching optical temporal decryption (OTD) module, and then injecting the signal emerging from the OTD module into a receiver ECSL to achieve original chaotic carrier synchronization for the final message decryption. It is shown that the proposed scheme can greatly enhance the bandwidth and efficiently suppress the TDS of original chaotic carrier. Moreover, it can also efficiently defense against the attacks of DLF and synchronization utilization, thus the proposed scheme provides considerably higher security with respect to the conventional ECSL-based chaotic communication systems. Finally, the use of transmission dispersion can be made in chaotic carrier decryption, and centralized secure wavelength division multiplexing (WDM) chaotic communications can also be achieved.

## 2. Theory and numerically modelling ~~model~~

Figure 1 shows the schematic of the proposed secure chaotic communication system. At the transmitter end, a conventional ECSL that is termed as master semiconductor laser (MSL) is adopted to provide an original chaotic carrier, and an optical intensity modulator is used to encrypt the message onto the original chaotic carrier. While significantly different from the conventional ECSL-based chaotic communication systems, in the proposed scheme, the modulated chaotic carrier (chaos + message) is sent to an OTE module for the carrier encryption instead of being directly transmitted to the receiver end. The OTE module is composed of one phase modulator (PM) driven by a secret key and a dispersion component ($D_E$). The aim of OTE is to hide the modulated chaotic carrier to avoid its direct exposure to the public. With the phase modulation, the spectrum of the modulated chaotic carrier is expanded greatly in the optical domain, and then the dispersion component converts the optical-spectrum-expanded phase chaos into intensity, leading to a greatly enhanced bandwidth and a flattened spectrum of the modulated chaotic carrier in the electronic domain.

On the other hand, due to the nonlinearity of the PM and the dispersion-associated nonlinear waveform distortion effect, the periodicity (induced by the linear feedback of the MSL) in the modulated chaotic carrier can be efficiently destructed, as such the TDS can be suppressed significantly. Technically speaking, with the OTE, the modulated chaotic carrier is encrypted as a totally different chaotic signal, this can greatly enhance the privacy of the chaotic carrier propagating over the public link. At the receiver end, the transmitted chaotic carrier firstly passes through an OTD module to decrypt the modulated chaotic carrier, after that, the recovered chaotic carrier is injected into a receiver ECSL referred to as slave semiconductor laser (SSL) to achieve chaos synchronization for the final message decryption. The configuration of the OTD module is similar to that of the OTE module, except that the signs of the secret PM driving signal and the coefficient of the dispersion component ($D_D$) are opposite to those of the OTE module. Since the signal transmitting over the public link is the OTE chaotic signal, the privacy of the modulated chaotic carrier is thus greatly enhanced. Under such a scenario, without applying a matching OTD module, the eavesdropper is not able to recover the modulated chaotic carrier, let alone to intercept the message. As a direct result, the information security is greatly enhanced. In addition, due to the fact that the phase modulators and dispersive components in the OTE and OTD modules ~~work~~ operate in a wide range of wavelength, the proposed system simultaneously supports centralized encryption/decryption ~~for~~ of several WDM channels ~~simultaneously~~. For ~~Under~~ such a scenario, the messages conveyed by ~~on~~ different chaotic communication channels are firstly embedded into the original chaotic carrier, and then the modulated chaotic carriers are multiplexed and sent through one OTE module. With the OTE module, the multiplexed WDM chaotic carrier would be encrypted as a compound signal for public link transmission. At the receiver end, the compound signal is firstly decrypted by the OTD module, and then the WDM modulated chaotic carriers (chaos + message) are derived from the decrypted signal and used for final message decryption.

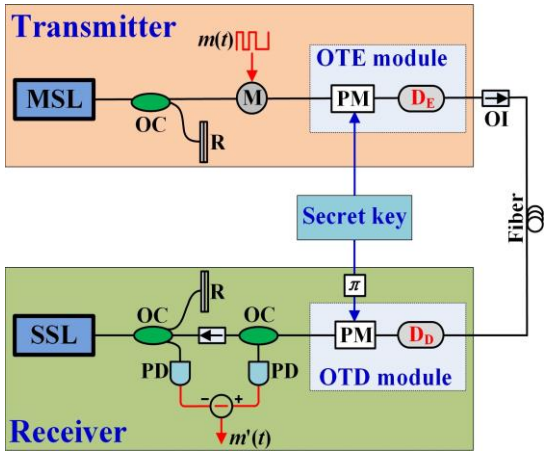


Fig. 1. Schematic of the proposed secure chaotic communication system with optical temporal encryption/decryption (OTE/D). MSL(SSL), master (slave) semiconductor laser; OC, optical coupler; R, reflector; M, intensity modulator; D, Dispersion component; PM, phase modulator; OI, optical isolator; PD, photodiode; m($t$), message; m'($t$), recovery message.

To numerically explore the dynamics of the ECSLs, the well-known Lang-Kobayashi rate equations are adopted, whose complex electric field amplitude $E(t)$ and the intra-cavity carrier number $N(t)$ of the MSL are written as [3-5, 19-21]

$$\frac{dE_m(t)}{dt} = \frac{1}{2}(1+i\alpha)[G_m(t) - \frac{1}{\tau_p}]E_m(t) + kE_m(t-\tau_f)\exp(-\omega_m\tau_f) + \sqrt{2\beta N_m(t)}\chi_m(t) \qquad (1)$$

$$\frac{dN_m(t)}{dt} = \frac{I}{q} - \frac{N_m(t)}{\tau_e} - G_m(t)\left|E_m(t)\right|^2 \tag{2}$$

While the rate equations for the SSL at the receiver end are written as

$$\frac{dE_s(t)}{dt} = \frac{1}{2}(1+i\alpha)[G_s(t) - \frac{1}{\tau_p}]E_s(t) + kE_s(t-\tau_f)\exp(-\omega_s\tau_f) + \sigma E_{inj}(t) + \sqrt{2\beta N_s(t)}\chi_s(t) \tag{3}$$

$$\frac{dN_s(t)}{dt} = \frac{I}{q} - \frac{N_s(t)}{\tau_e} - G_s(t)\left|E_s(t)\right|^2 \tag{4}$$

$$G_{m,s}(t) = \frac{g[N_{m,s}(t) - N_0]}{1 + \varepsilon\left|E_{m,s}(t)\right|^2} \tag{5}$$

In these equations, the subscripts *m* and *s* denote the MSL and SSL, respectively. $E_{inj}(t)$ is the injected chaotic carrier that is recovered by the OTD module after transmitting over the public link. $G(t)$ denotes the optical gain which is defined as Eq. (5). $I$ is the injection current, $q$ is the electron charge. The other intrinsic parameters include the linewidth enhancement factor $\alpha$, the angle frequency $\omega$, the carrier lifetime $\tau_e$, the photon lifetime $\tau_p$, the spontaneous emission rate $\beta$, the carrier number at transparency $N_0$, the differential gain coefficient $g$, and the gain saturation factor $\varepsilon$. $k$ and $\tau_f$ are the feedback strength and delay, respectively, and $\sigma$ is the injection strength. The unity-variance and zero-mean Gaussian noise source $\chi(t)$ is introduced to model the spontaneous emission noise [18].

In the OTE module, phase modulation can be performed by a typical electro-optical phase modulator such as a QPSK modulator. Here for the proof-of-concept demonstration, we choose one typical $LiNiO_3$ phase modulator, which is mathematically described as

$$E_{out}(t) = E_{in}(t)\exp(i\pi\frac{V_{key}(t)}{V_\pi}) \tag{6}$$

where the subscripts "in" and "out" denote the input and output of the PM, respectively. The PM driving signal is a secret key for both the OTE and the OTD, it is a radio frequency sinusoidal signal that is mathematically described as $V_{key}(t)=A_0\cos(2\pi f_0 t)$, where $A_0$ and $f_0$ stand for the amplitude and the frequency of the secret key signal, respectively. The dispersion component $D_E$ can be constructed with a dispersive fiber or a chirped fiber Bragg grating (CFBG). For simplicity, we take a dispersive fiber here. When excluding the higher order dispersions, the transfer function of the dispersive fiber in the frequency domain can be written as [20, 22]

$$H_{DE}(\omega) = K_1\exp(i\frac{1}{2}\beta_{2E}L_E\omega^2) \tag{7}$$

where $K_1$ is a constant, $L$ is the length of the dispersive fiber, $\beta_{2E}=-D_E\lambda^2/2\pi c$ denotes the group velocity dispersion, $\lambda$ is the wavelength of the chaotic carrier and $c$ is the velocity of light in vacuum. Applying the inverse Fourier transformation to Eq. (7), we can obtain the pulse response in the time domain

$$h_{DE}(t) = F^{-1}[H_{DE}(\omega)] = K_2\exp(-i\frac{\omega_0}{2\lambda_0 D_E L_E}t^2), \tag{8}$$

where $F^{-1}$ means the inverse Fourier transformation, and $K_2$ is a constant associated with $\beta_{2E}L_E$.

The transmission link consists of a standard single mode fiber (SMF), which can be described by the following nonlinear Schrödinger equation [14, 23]

$$i\frac{\partial E_t}{\partial z} = -\frac{i}{2}\alpha_F E_t - \gamma\left|E_i\right|^2 E_t + \frac{1}{2}\beta_{2F}\frac{\partial^2 E_t}{\partial t^2} + \frac{i}{6}\beta_{3F}\frac{\partial^3 E_t}{\partial t^3} \tag{9}$$

where $E_t$ is the envelop of the electric field of the OTE chaotic carrier, $\alpha_F$ is the loss coefficient of the SMF, $\gamma$ is the nonlinear coefficient of the SMF, $\beta_{2F}$ and $\beta_{3F}$ are the second-order and the third-order chromatic dispersions, respectively.

The configuration of the OTD module is a symmetric replica with respect to the OTE module, while the amplitude of the key signal is inverse to that of the OTE module, which can be described as $V'_{key}(t)=-A_0\cos(2\pi f_0 t)$. The dispersion coefficient ($D_D$) and the length ($L_D$) of the dispersive fiber in the OTD module satisfy the following condition:

$$D_E L_E + D_F L_F + D_D L_D = 0 \tag{10}$$

where $D_F=-\beta_{2F}2\pi c/\lambda^2$ and $L_F$ are the dispersion coefficient and the length of the SMF link, respectively. Here the transmission dispersion is considered in the OTD module, as such no additional transmission dispersion compensation is needed. In fact, the transmission fiber can also be considered as a second cascaded dispersive component of the OTE module, and then Eq. (10) sets ~~is~~ the essential conditions for the ~~achievement of~~ OTD module having an inverse process ~~.which is the inverse transformation of OTE.~~

To quantify the correlation and synchronization quality of the chaotic signals in the proposed system, we define the cross-correlation function (CCF) of the intensities of chaotic carriers as [22, 24-26]

$$C_{XY}(\Delta t)=\frac{\left\langle [I_X(t)-\langle I_X(t)\rangle]\cdot[I_Y(t-\Delta t)-\langle I_Y(t)-\Delta t\rangle]\right\rangle}{\sqrt{\left\langle [I_X(t)-\langle I_X(t)\rangle]^2\right\rangle\cdot\left\langle [I_Y(t-\Delta t)-\langle I_Y(t)-\Delta t\rangle]^2\right\rangle}} \tag{11}$$

where $I(t)$ is the intensity of a chaotic carrier, the subscripts $X$, $Y$ represent two different chaotic carriers in the system, the operation <·> means time averaging, and $\Delta t$ is the time that $I_Y(t)$ is shifted with respect to $I_X(t)$. This equation can also be used to calculate the autocorrelation function (ACF) by setting $I_X(t)=I_Y(t)$.

To numerically investigate the proposed system, the fourth order Runge-Kutta algorithm is adopted to solve the rate equations, and the split-step Fourier method is used to solve the nonlinear Schrödinger equation. Unless otherwise stated, the values of the parameters used in the simulations are listed in Table I. In the section below, we numerically investigate the properties of the optical temporal encryption and those of the chaos synchronization and communication.

Table 1. Values of parameters used in the simulations [13, 14, 20]

| Symbol | Parameter | Value |
|---|---|---|
| $I_{th}$ | Threshold current | 14.7 mA |
| $I$ | Bias current of MSL and SSL | $1.5I_{th}$ |
| $\lambda$ | Operation wavelength | 1550 nm |
| $\alpha$ | Linewidth enhancement factor | 5 |
| $\tau_e$ | Carrier lifetime in SL active region | 2ns |
| $\tau_p$ | Photon lifetime in SL active region | 2ps |
| $\beta$ | Spontaneous emission rate | $1\times10^{-6}$ ns$^{-1}$ |
| $N_0$ | Transparency carrier number | $1.5\times10^{8}$ |
| $g$ | Differential gain coefficient | $1.5\times10^{-8}$ ps$^{-1}$ |
| $\varepsilon$ | Gain saturation factor | $5\times10^{-7}$ |
| $k$ | Feedback strength | 15 ns$^{-1}$ |
| $\tau_f$ | Feedback delay | 3 ns |
| $\sigma$ | Injection strength | 80 ns$^{-1}$ |
| $L_E$ | Length of dispersive fiber in OTE module | 3 km |
| $D_E$ | Dispersion coefficient of dispersive fiber in OTE module | 500 ps/nm/km |
| $K_1$ | Constant factor of transfer response of dispersive fiber | 1 |
| $A_0$ | Amplitude of secret key | $V_\pi$ |
| $f_0$ | Frequency of secret key | 9.1 GHz |
| $\alpha_F$ | Loss coefficient of fiber link | 0.2 dB/km |
| $\beta_{2F}$ | Velocity dispersion of single mode fiber | 20.4 ps$^2$/ km |
| $\beta_{3F}$ | Third-order dispersion of fiber link | 0.1ps$^3$/km |
| $L_F$ | Length of transmission single-mode fiber | 50 km |

## 3. Properties of optical temporal encryption

Figure 2 shows the intensity waveforms, RF spectra and ACF curves of the original chaotic carrier and the encrypted chaotic signal, in the absence of message transmission. It can be seen that the original chaotic carrier generated by the MSL ($I_M(t)$) is encrypted as a totally different signal. The OTE chaotic signal ($I_{OTE}(t)$) shows a significantly flattened spectrum having a wide bandwidth with respect to the original chaotic carrier. By examining the efficient bandwidths of these two chaotic signals, it is found that the efficient bandwidth of the chaotic carrier is expanded from the original 11.5 GHz to 49.4 GHz, indicating that the bandwidth of the original chaotic carrier is enhanced by more than 3 times. Here the efficient bandwidth is defined as the span between the direct current (DC) and the frequency where 80% of energy is contained in the RF spectrum [16, 20, 27]. It is also worth noting that the dips in the RF spectrum of the OTE chaotic carrier is attributed to the chromatic dispersion-induced power fading effect, as theoretically analyzed in [28]. On the other hand, as shown in Figs. 2(c) and 2(f), the TDS in the original chaotic carrier is also efficiently compressed by the OTE module, this means the complexity of the chaotic carrier is also greatly enhanced. The excellent TDS compression feature can minimize the risk that any eavesdroppers use the ACF-enabled feedback delay to reconstruct a similar ECSL system to intercept the message, in virtue of the synchronization utilization attack.

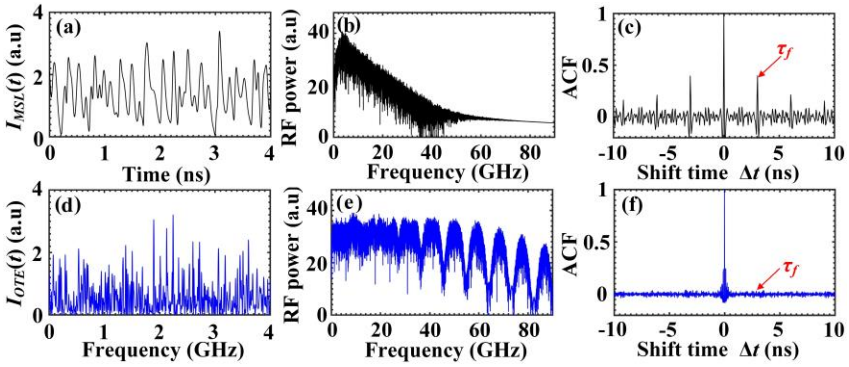


Fig.2. Temporal waveform, RF spectrum, and ACF of the original and encrypted chaotic carrier.

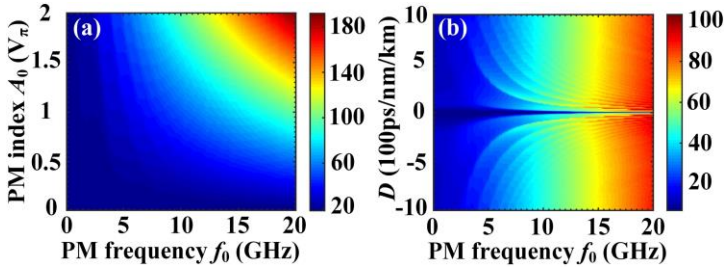


Fig.3. (a) Efficient bandwidth EB (GHz) of OTE chaotic carrier versus the index $A_0$ and frequency $f_0$ of phase modulation; (b) EB (GHz) of OTE chaotic carrier in the space of the dispersion coefficient $D$ and the PM frequency $f_0$, for the case of $A_0=V_\pi$.

To further investigate the influence of the OTE on the original chaotic signal, the efficient bandwidth and TDS characteristics of the encrypted chaotic signal are further systematically investigated. Figure 3(a) shows the variation of the efficient bandwidth of the encrypted chaotic signal as a function of amplitude ($A_0$) and frequency ($f_0$) of the key signal. It is seen that the efficient bandwidth of the OTE chaotic signal is monotonically enhanced as the increase of $A_0$ and $f_0$. Figure 3(b) shows the influences of the dispersion coefficient $D$ and the PM frequency $f_0$ on the efficient bandwidth of the OTE chaotic carrier, for the case of $A_0=V_\pi$.

It is shown that as the absolute value of the dispersion coefficient is larger than 10 ps/nm/km, it is easy to obtain a wideband bandwidth OTE chaotic carrier with a high PM frequency, and similar to that in Fig. 3(a), the efficient bandwidth of the OTE chaotic signal is also monotonically enhanced with increasing PM frequency. The OTE-induced bandwidth enhancement is originated from the spectrum expansion effect of PM. The instantaneous frequency offset derived from the phase modulation expressed in Eq. (6) is determined by

$$\Delta f_{PM}(t) = -A_0 f_0 \sin(2\pi f_0 t) \tag{12}$$

thus, the maximum frequency offset that is closely related to the bandwidth of the OTE chaotic carrier is approximately

$$\left|\Delta f_{PM}\right|_{\max} = A_0 f_0 \tag{13}$$

It is clear that, when $f_0$ ($A_0$) is fixed, $|\Delta f_{PM}|_{\max}$ monotonically increases with increasing $A_0$ ($f_0$). The increase in $|\Delta f_{PM}|_{\max}$ allows that the bandwidth enhancement of the OTE chaotic carrier. These discussions indicate that, with the proposed OTE scheme, the efficient bandwidth of the chaotic carrier can be expanded significantly. Bandwidth of the OTE chaotic carrier beyond 100GHz is achievable when sufficiently large values of $A_0$, $f_0$, and $D$ are adopted.

On the other hand, Fig. 4 shows the variations of the TDS of the OTE chaotic carrier, in the spaces of ($A_0$, $f_0$) and ($D$, $f_0$). Here the TDS is defined as the maximum ACF value nearby the position of feedback delay in the ACF curve. Figure 4(a) shows that, with a PM index larger than 0.3 and a PM frequency higher than 5 GHz, it is easy to suppress the TDS toward an indistinguishable level close to 0. Similarly, in Fig. 4(b), it is shown that the higher the PM frequency and the larger the dispersion coefficient, the easier the TDS can be suppressed toward a level close to 0. Nevertheless, it is worth mentioning that, to efficiently suppress the TDS of the chaotic carrier, the value of $f_0$ should not be an integral multiple of the external-cavity resonation frequency ($1/\tau_f$). This is because when the value of $f_0$ is an integral multiple of $1/\tau_f$, the phase modulation frequency is harmonic to the external cavity resonance frequency, as such the phase modulation in the OTE module cannot efficiently destruct the periodicity induced by the linear external cavity optical feedback.

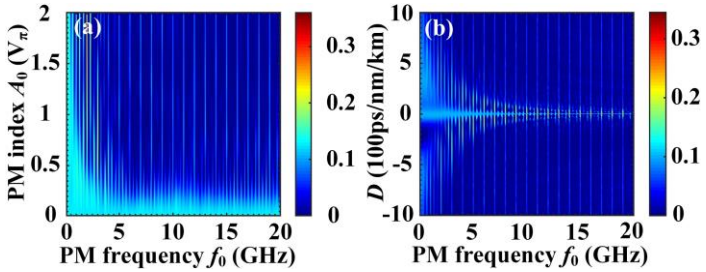


Fig.4. (a) TDS value in ACF of OTE chaotic carrier versus the PM index $A_0$ and frequency $f_0$; (b) TDS value in ACF of OTE chaotic carrier in the space of the dispersion coefficient $D$ and the PM frequency $f_0$, for the case of $A_0$=$V_\pi$.

In general, based on the joint effects of the spectrum expansion of phase modulation and the phase-to-intensity conversion of the dispersion component in the OTE module, conventional original chaotic signal can be encrypted as a totally uncorrelated flat-spectrum wideband chaotic signal with indistinguishable TDS. Based on such properties, the privacy of the original chaotic carrier can be greatly enhanced in both the time domain and the frequency domain.

## 4. Chaos synchronization and message transmission

In this section we focus on the properties of chaos synchronization and the secure message transmission. As already stated, at the receiver end, the encrypted chaotic carrier is firstly decrypted by a matching OTD module. The PM driving signal in the OTD module is the

inverse-phase replica of that in OTE module, and the coefficient of the OTD dispersion unit $D_D$ is determined by Eq. (10). After that, the decrypted chaotic carrier is sent into the SSL to achieve original chaotic carrier synchronization for the final message decryption.

### *4.1 Performance of chaotic carrier synchronization*

Figure 5 shows the intensity waveforms of the original chaotic carrier outputted by the MSL ($I_{MSL}(t)$), the OTE chaotic signal ($I_{OTE}(t)$), the corresponding OTD chaotic carrier ($I_{OTD}(t)$), the receiver-end local chaotic carrier generated by SSL ($I_{SSL}(t)$), as well as the pairwise cross-correlations between the original chaotic carrier and the other three chaotic signals. The CCF curve in Fig. 5(e) shows that the correlation coefficient between the OTE chaotic signal and the original chaotic carrier is smaller than 0.04, this means that the cross correlation between them is very weak. The original chaotic carrier is, therefore, encrypted as a totally uncorrelated signal, this agrees with the phenomenon shown in Fig. 2. Based on this property, the privacy of the original chaotic carrier can be guaranteed by transmitting the OTE chaotic carrier over the public fiber link. On the other hand, the comparison between the OTD chaotic signal in Fig. 5(c) and the original chaotic carrier in Fig. 5(a) indicates that the original chaotic carrier is successfully decrypted by the OTD module from the link-transmission signal, this can also be confirmed by the CCF curve in Fig. 5(f), where a cross correlation coefficient of 0.99 between the OTD chaotic carrier and the original chaotic carrier is observed. Due to the dispersion and nonlinearity of the fiber link, some high-frequency small-amplitude jitters appear in the OTD chaotic carrier, this induces negligible distortions, with respect to the original chaotic carrier. Nevertheless, with the low-pass filtering effect of the SSL and the injection-locking effect, the transmission distortion does not induce any obvious degradations in chaos synchronization between the SSL and the MSL. As shown in Fig. 5(g), the local chaotic carrier can be well synchronized with the original chaotic carrier with a correlation coefficient of 0.99.

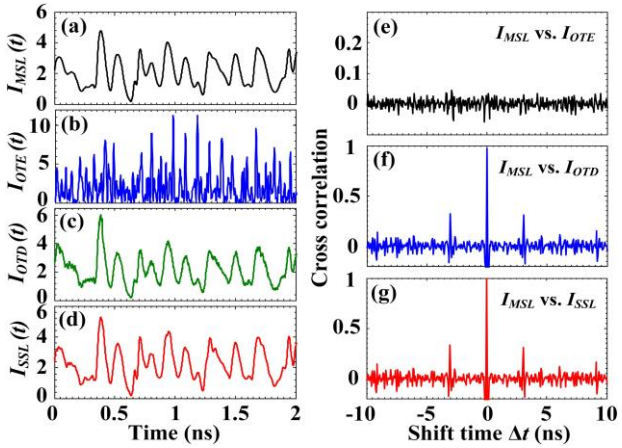


Fig.5. Temporal intensities of (a) original chaotic carrier, (b) OTFE chaotic carrier, (c) OTFD chaotic carrier, and d local chaotic carrier generated by SSL. (e)–(g) the cross-correlations between original chaos and the other three chaotic signals.

Figure 6(a) shows the synchronization quality between the original chaotic carrier and the local chaotic carrier versus the injection strength in the proposed system and the conventional system without incorporating the OTE/OTD. It is shown that the performance of the proposed system is similar to that of the conventional system. With sufficiently strong injection, high

quality chaos synchronization can be easily achieved. On the other hand, Fig. 6(b) shows the comparison of mismatch robustness properties between the proposed system and the conventional system. The mismatch is introduced using the method reported in [29, 30]. The results indicate that the OTE and OTD processes in the proposed system do not induce obvious mismatch robustness degradation with respect to that in the conventional systems. Therefore, it can be concluded that in the proposed system, the OTE and OTD processes do not induce considerable synchronization performance degradation for the chaotic carriers.

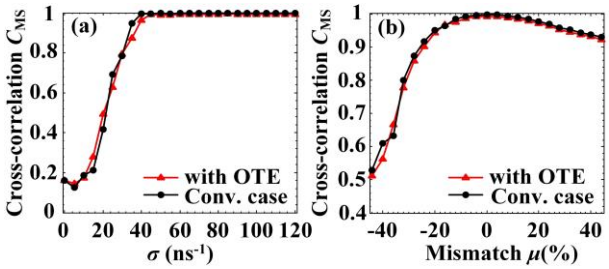


Fig. 6. Comparison of chaos synchronization quality versus (a) injection strength and (b) parameter mismatch in the proposed system (triangle) and conventional system without OTE/OTD (circle).

### *4.2 Performance of chaotic communication*

By making use of the high-quality chaos synchronization, we investigate the secure chaotic communication in the proposed system. The message encryption is performed by the method of chaos modulation, which can be mathematically described as $I_{mod}(t)=I_{MSL}(t)[1+A_m \cdot m(t)]$, where $I_{mod}(t)$ denotes the intensity of the modulated chaotic carrier, the message $m(t)$ is a random binary sequence, and $A_m=0.1$ is the modulation index [20, 30, 31]. The message decryption is carried out by the way of direct subtraction decoding, which is described as $m'(t)=LPF[I_{OTD}(t)-I_{SSL}(t)]$. Here the LPF operation uses a five-order Butterworth low-pass-filter with a cutoff frequency equal to the message bit rate $R$. To quantify the system performance, the bit-error-ratio (BER) of the decrypted message is evaluated by [32]

$$BER = \frac{\exp(-Q^2/2)}{\sqrt{2\pi}Q} \tag{14}$$

where $Q$ is the Q-factor of the recovered message, which is defined as

$$Q = \frac{I_1 - I_0}{\sigma_1 + \sigma_0} \tag{15}$$

where $I_1$ and $I_0$ stand for the average power of bits "1" and "0", respectively; while $\sigma_1$ and $\sigma_0$ are their corresponding standard deviations.

Figure 7 shows the temporal waveforms of the original messages and their corresponding decrypted messages, as well as the corresponding eye diagrams of the decrypted messages, for three-channel WDM communication systems with $R$=2 Gbit/s. Here the WDM channels are centralized at 1550 nm with a channel spacing of 0.8 nm (100 GHz), namely $\lambda_{-1}$=1549.2 nm, $\lambda_0$=1550 nm, $\lambda_{+1}$=1550.8 nm. Clearly, the messages transmitted on all the WDM channels are correctly recovered, and the widely-open eye diagrams also mean low BERs of the decrypted message.

To further investigate the communication performance of the proposed system, the solid curves in Fig. 8 show the BER performance of legal communication versus the bit rate of the message $R$. It is shown that although the BER performance degrades as the increase of message bit rate, an acceptable communication performance with a BER lower than $10^{-6}$ can be achieved when the bit rates of channel $\lambda_{-1}$, channel $\lambda_0$ and channel $\lambda_{+1}$ are lower than 4.5 Gbit/s, 6 Gbit/s and 4.5Gbit/s, respectively. The BER performances on the side-wavelength

channels (the triangle curves) are similar and worse than that of the central-wavelength channel. The BER degradation on the side-wavelength channels here is attributed to the dispersion considered in $D_D$ of the OTD module (see Eq. 10) is evaluated according to the transmission dispersion on the central wavelength channel $\lambda_0$. For the side-wavelength channels, the dispersion amounts considered in $D_D$ is not as accurate as the actual transmission dispersions experienced by these channels, as such, the transmission dispersions cannot be compensated completely. Consequently, the decryption performances of these channels are degraded because of the residual transmission dispersion-induced distortion. It is worth mentioning that due to the channel cross-talk, the BER performance of WDM communication is slightly worse than that of the single channel transmission scenario (solid-circle).

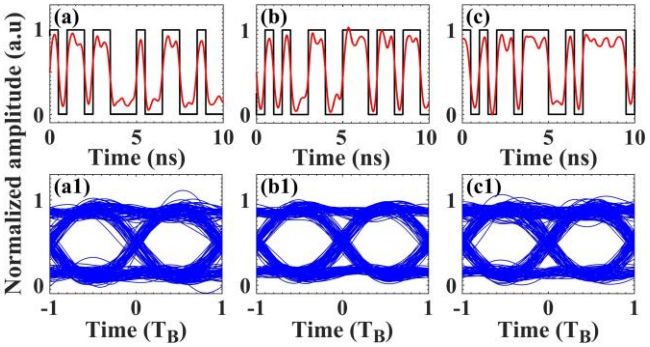


Fig. 7. Illustration of WDM message encryption/decryption processes. (a), (b), (c) show the original messages (dashed) and recovery messages (solid) on the three channels of $\lambda_{-1}$=1549.2 nm, $\lambda_0$=1550 nm, $\lambda_{+1}$=1550.8 nm, for the cases with bit rates of 2 Gbit/s, respectively, while (a1), (b1), (c1) show the corresponding eye diagrams.

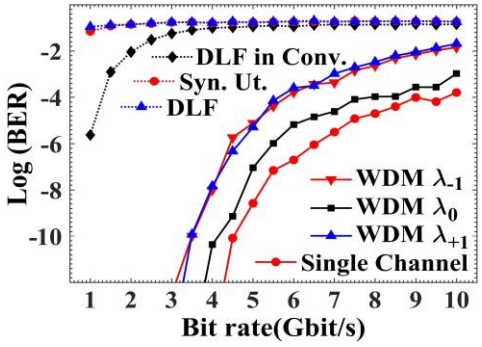


Fig. 8. Performance (Log(BER)) of the legal decryption (solid), the illegal interception from the original modulated chaotic carrier by DLF (dashed-diamond), the interception from the OTE chaotic carrier by DLF (dashed-triangle), and the interception by the synchronization utilization method (dashed-circle)

## 5. Security analysis

In this section, the security of message transmission in the proposed system is discussed. On one hand, the system security under the typical blind attack scenarios occurring on the public link, namely DLF and synchronization utilization, as mentioned above, are considered. On the other hand, the physical key space of the OTE is investigated. For the sake of simplicity, only the single channel transmission scenario ($\lambda$=$\lambda_0$=1550 nm) is discussed in this section. However, it is reasonable to expect that the system security under the centralized WDM communication scenario can be further enhanced with respect to the single channel scenario. This is because it is extremely difficult for the eavesdropper to obtain correct chaotic carriers

from the compound signal transmitted over the public channel, without matching the OTD module and precise wavelength de-multiplexer or optical filters.

### 5.1 Security under blind link attacks

The DLF is the most straightforward attack way of intercepting messages from public fiber links. Under this scenario, the eavesdropper adopts a low-pass filter to intercept the message directly from the public link. In our simulations, a five-order Butterworth low-pass filter with a cutoff frequency equal to the message bit rate $R$ is used to directly intercept the message from the fiber link between the MSL and the SSL. In Fig. 8, the dashed-circle and dashed-diamond curves show the BERs of the message intercepted by DLF from the original modulated chaotic carrier and the OTE chaotic carrier. Obviously, the BERs of the intercepted messages in the proposed system are too high for the eavesdropper to obtain correct message. Moreover, with respect to the BER of the intercepted message in the conventional system without OTE, the BER in the proposed system is much higher. In the conventional system, when the bit rate is 1 Gbit/s, the message can be illegally decrypted with a BER lower than $10^{-5}$, it cannot defend the DLF attack. While in the present system, the BER of the intercepted message is about 0.08, it is difficult for the eavesdropper to correctly recover the original message. These results indicate that with the OTE, the message can be more efficiently hidden in the link chaotic carrier, and the proposed system can successfully defend against the DLF attack, even when the bit rate of message is low.

Regarding the attack of synchronization utilization, we consider the most serious case, in which the eavesdropper is equipped with an attack laser (SLA) that is an ECSL identical to the MSL and the SSL. The OTE chaotic carrier transmitted on the public link is split, amplified and then injected into the SLA to achieve chaos synchronization for the illegal message decryption. The injection strength is set as 80 $ns^{-1}$ as that of the legal decryption to obtain high quality chaos synchronization. The dashed-triangle curve in Fig. 8 shows the BER variation of the intercepted message under this type of attack versus the message bit rate. Apparently, with respect to the legal decryption (solid circle curve), the BER of the intercepted message is always maintained at a very high level. Even in the low bit rate transmission case of $R$=1 Gbit/s, the BER of the intercepted message under this attack is larger than 0.1. Therefore, the proposed scheme can also defend against the attack of synchronization utilization.

In summary, in the proposed system, it is difficult for the eavesdropper to intercept the correct message from the chaotic carrier transmitted over the public fiber link. Comparing with the conventional chaotic communication scheme without OTE, the proposed system can significantly enhance the security against the public link attacks.

### 5.2 Physical key space analysis

In the proposed system, due to the introduction of the OTE, the mismatch sensitivity of the control parameters, namely the amplitude $A_0$ and the frequency $f_0$ of the PM driving signal, as well as the dispersion coefficients ($D_E$ and $D_D$ in Eq. (10)), is also an important factor determining the system security. Since they are physical parameters of hardware, we refer them to as the physical keys, which are different from the keys in the conventional cryptography system where the keys are generated by algorithms rather than physical signals. Based on the key space analysis method in [33], the physical key space is determined by the tuning ranges and the mismatch resolutions of the tunable parameters of the PM and dispersive component, namely $A_0$, $f_0$ and $D$.

Figure 9 shows the influences of the parameter mismatches of the PM driving signal on the BER of the decrypted message, for a bit rate of 5 Gbit/s. From the perspective of the common commercial availability, the maximum tuning range of $A_0$ is set as $4V_\pi$, and 40GHz for $f_0$. The

mismatch resolution is defined as the critical mismatch point where the BER of the recovered message corresponds to 0.1, which is large enough to guarantee that no useful message can be recovered. As shown in Fig. 9(a), the BER performance degrades gradually, as the increase of the mismatch of $A_0$, and a mismatch about $0.4V_\pi$ causes a BER larger than 0.1. Moreover, Fig. 9(b) shows that the BER is sensitive to the mismatch of $f_0$. A frequency mismatch as small as about 150 kHz would cause the BER to rapidly increase to 0.1. Therefore, the private PM can contribute a physical key space about $2.67\times10^6$ ($4V_\pi/0.4V_\pi\times40$GHz/150kHz) to the security system. It is also worth mentioning that the key space can be further enlarged by increasing the number of PMs or using high-speed modulator in the OTE module.

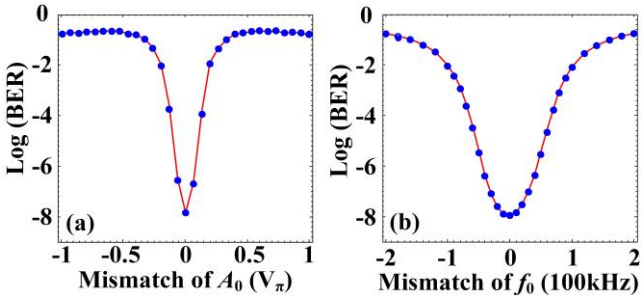


Fig. 9. Sensitivity of BER to the mismatches of (a) PM index $A_0$ and (b) PM frequency $f_0$. Here the message bit rate is chosen as $R$=5Gbit/s.

Figure 10 shows the influence of the mismatch of dispersion coefficient on the BER performance. Here, the value of $D_E$ is fixed, while $D_D$ is mismatched from its optimum value determined by Eq. (10). It is shown that a mismatch resolution about 15ps/nm/km would degrade the BER to a threshold level of 0.1. If the dispersion unit is an optical fiber, there is an infinite key space, as long as the fiber is sufficiently long (here the transmission loss of fiber is not considered, since it can be effectively compensated by ~~with~~ optical amplifiers, such as EDFAs and SOAs). If a pair of tunable chirped fiber Bragg gratings (CFBG) with a tuning range from -2000 ps/nm to 2000 ps/nm are adopted in the OTE module and the OTD module, an additional key space about 89 [4000ps/nm/(15ps/nm/km×3km)] can be contributed to the proposed system. Consequently, the total physical key space is enhanced to $2.37\times10^8$ ($2.67\times10^6\times89$). It is worth noting that the physical key space of the proposed system can be exponentially enhanced by cascading the dispersion units (dispersion fibers or CFBGs) in the OTE and OTD modules. When $n$ pair of matching cascaded OTE and OTD modules are applied in the proposed scheme, the resulting physical key space would be $(2.37\times10^8)^n$.

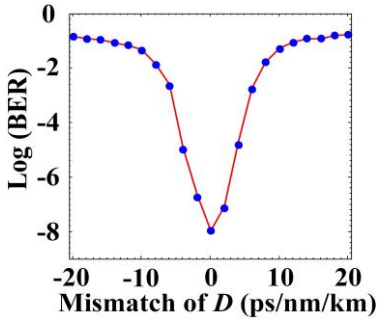


Fig. 10. Sensitivity of BER to the mismatch of dispersion coefficient $D$. here the parameters are identical to those in Fig. 9.

## 6. Conclusions

We have numerically demonstrated a physical security-enhanced chaotic communication scheme by encrypting the modulated chaotic carrier temporally. In the proposed system, rather than directly propagating through a public link, the modulated chaotic carrier is firstly encrypted as an uncorrelated chaotic signal and then transmitted to the receiver end. The numerical results have indicated that with the OTE the efficient bandwidth of the original chaotic carrier can be expanded by several times and the TDS in the original chaotic carrier can also be completely suppressed, and the OTE chaotic carrier is fully uncorrelated with the original chaotic carrier, these properties greatly enhance the privacy of the chaotic carrier. With a matching OTD module, the original chaotic carrier can be successfully decrypted, and high-quality chaotic carrier synchronization can be achieved, which supports centralized WDM message encryption and decryption at several Gbit/s, without any dispersion compensation. The proposed system can efficiently defend against typical blind attacks that threaten the security of conventional chaotic communication configurations. Moreover, the communication performance is sensitive to the parameter mismatches between the OTE and OTD modules, this provides an additional large physical key space for the security system, and the security can be exponentially increased by cascading the OTE modules. The proposed scheme paves a solid path leading to its implementation in high-security optical chaotic communication systems.


## Funding

National Science Foundation of China (NSFC) (61671119, 61471087); 111 Project (B14039).


## References


1. L. M. Pecora, T. L Carroll., "Synchronization in chaotic systems," Phys. Rev. Lett. **64**(8), 821-825 (1990).
2. M. Sciamanna, K. A. Shore, "Physics and applications of laser diode chaos," Nature Photon. **9**(3), 151-162(2015).
3. N. Q. Li, H Susanto, B. Cemlyn, I. D. Henning, M. J. Adams, "Secure communication systems based on chaos in optically pumped spin-VCSELs," Opt. Lett. **42**(17), 3494-3497 (2017).
4. T. Deng, G. Q. Xia, Z. M Wu, "Broadband chaos synchronization and communication based on mutually coupled VCSELs subject to a bandwidth-enhanced chaotic signal injection," Nonlinear Dyn. **76**(1), 399–407 (2014).
5. Y. Fu., M. Cheng, X. Jiang, L. Deng, C. Ke, S. Fu, M. Tang, M. Zhang, P. Shum, D. Liu, "Wavelength division multiplexing secure communication scheme based on an optically coupled phase chaos system and PM-to-IM conversion mechanism," Nonlinear Dyn. **94**(3): 1949-1959 (2018).
6. P. Li, K. Li, X. Guo, Y. Guo, Y. Liu, B. Xu, A. Bogris, K. A. Shore, and Y. Wang, "Parallel optical random bit generator," Opt. Lett. **44**(10), 2446-2449 (2019).
7. N. Q. Li, B. Kim, V. N. Chizhevsky, A. Locquet, M. Bloch, D. S. Citrin, W. Pan, "Two approaches for ultrafast random bit generation based on the chaotic dynamics of a semiconductor laser," Opt. Express **22**(6), 6634-6646 (2014).
8. N. Q. Li, W. Pan, S. Xiang, B. Luo, L. Yan, X. Zou, "Hybrid chaos-based communication system consisting of three chaotic semiconductor ring lasers," Applied Optics **52**(7), 1523-1530 (2013).
9. C. Xue, N. Jiang, Y. Lv, K. Qiu, "Secure key distribution based on dynamic chaos synchronization of cascaded semiconductor laser systems," IEEE Trans. on Commun. **65**(1), 312-317 (2017).
10. A. Argyris, D. Syvridis, L. Larger, V. Annovazzi-Lodi, P. Colet, I. Fischer, J. García-Ojalvo, C. R. Mirasso, L. Pesquera, K. A. Shore, "Chaos-based communications at high bit rates using commercial fiber-optic links" Nature **437**(17), 343–346 (2005).
11. Y. H. Hong, K. A. Shore, "Power loss resilience in laser diode-based optical chaotic communications systems," J. Lightw. Technol. **28**(3), 270-276(2010).
12. D. Kanakidis, A. Argyris, A. Bogris, D. Syvridis, "Influence of the decoding process on the performance of chaos encrypted optical communication systems," J. Lightw. Technol. **24**(1), 335-341 (2006).
13. A. Bogris, A. Argyris, D. Syvridis, "Encryption efficiency analysis of chaotic communication systems based on photonic integrated chaotic circuits," IEEE J. Quantum Electron. **46**(10), 1421-1429 (2010).
14. N. Jiang, C. Zhang, K. Qiu, "Secure passive optical network based on chaos synchronization," Opt. Lett. **37**(21), 4501–4503 (2012).

15. D. Rontani, A. Locquet, M. Sciamanna, D. S. Citrin, S. Ortin, "Time-delay identification in a chaotic semiconductor laser with optical feedback: a dynamical point of view," IEEE J. Quantum Electron. **45**(7), 879–891 (2009).
16. A. Wang, Y. Yang, B. Wang, B. Zhang, L. Li, Y. Wang, "Generation of wideband chaos with suppressed time-delay signature by delayed self-interference," Opt. Express **21**(7), 8701–8710 (2013).
17. S. Xiang, A. Wen, W. Pan, L. Lin, H. Zhang, X. Guo, J. Li, "Suppression of chaos time delay signature in a ring network consisting of three semiconductor lasers coupled with heterogeneous delays," J. Lighw. Technol. **34**(18), 4221–4227, (2016).
18. T. Heil, I. Fischer, W. Elsasser, J. Mulet, C. R. Mirasso, "Chaos synchronization and spontaneous symmetry-breaking in symmetrically delay-coupled semiconductor lasers," Phys. Rev. Lett. **86**(5), 795–798 (2001).
19. R. Lang, K. Kobayashi, "External optical feedback effects on semiconductor injection laser properties," IEEE J. Quantum Electron. **16**(3), 347–355 (1980).
20. N. Jiang, C. Wang, C. Xue, G. Li, S. Lin, K. Qiu, "Generation of flat wideband chaos with suppressed time delay signature by using optical time lens," Opt. Express **25**(13), 14359-14367(2017).
21. N. Q. Li, R. M. Nguimdo, A. Locquet, D. S. Citrin, "Enhancing optical-feedback-induced chaotic dynamics in semiconductor ring lasers via optical injection," Nonlinear Dyn. **92**(2), 315–324 (2018).
22. M. Cheng, L. Deng, H. Li, D. Liu, "Enhanced secure strategy for electro-optic chaotic systems with delayed dynamics by using fractional Fourier transformation," Opt. Express **22**(5), 5241–5251 (2014).
23. F. Zhang, P. L. Chu, "Effect of transmission fiber on chaotic communication system based on erbium-doped fiber ring laser," J. Lightw. Technol. **21**(12), 3334–3343(2003).
24. N. Jiang, C. Xue, Y. Lv, K. Qiu, "Physical enhanced secure wavelength division multiplexing chaos communication using multimode semiconductor lasers," Nonlinear Dyn. **86**(3), 19387-1949 (2016).
25. J. G. Wu, Z. M. Wu, Y. R. Liu, L. Fan, X. Tang, G. Q. Xia, "Simulation of bidirectional long-distance chaos communication performance in a novel fiber-optic chaos synchronization system," J. Lightw. Technol. **31**(3), 461-467 (2013).
26. S. Xiang, W. Pan, L. Yan, B. Luo, X. Zou, N. Jiang, L. Yang, "Impact of unpredictability on chaos synchronization of vertical-cavity surface-emitting lasers with variable-polarization optical feedback," Opt. Lett. **36**(17), 3497-3499 (2011).
27. Y. H. Hong, P. S. Spencer, K. A. Shore, "Wideband chaos with time-delay concealment in vertical-cavity surface-emitting lasers with optical feedback and injection," IEEE J. Quantum Electron., **50**(4), 236-242(2014).
28. Y. Gao, Q. Zhuge, W. Wang, X. Xu, J. M. Nuset, M. Morsy-Osman, M. Chagnon, F. Li, L. Wang, C. Lu, A. P. T. Lau, D. V. Plant, "Nonlinear dynamical characteristics of an optically injected semiconductor laser subject to optoelectronic feedback," Opt. Comun. **221**(1-3), 173-180 (2003).
29. N. Jiang, A. K. Zhao, S. Q. Liu, C. P. Xue, K. Qiu, "Chaos synchronization and communication in closed-loop semiconductor lasers subject to common chaotic phase-modulated feedback," Opt. Express **26**(25), 32404-32416 (2018).
30. A. Bogris, P. Rizomiliotis, K. E. Chlouverakis, A. Argyris, D. Syvridis, "Feedback phase in optically generated chaos: a secret key for cryptographic application," IEEE J. Quantum Electron. **44**(2), 119-124 (2008).
31. D. Kanakidis, A. Argyris, A. Bogris, D. Syvridis, "Influence of the decoding process on the performance of chaos encrypted optical communication system," J. Lightw. Technol. **24**(1), 335-341 (2006).
32. F. Zhang, P. L. Chu, "Effect of transmission fiber on chaotic communication system based on erbium-doped fiber ring laser," J. Lightw. Technol. **21**(12), 3334–3343 (2003).
33. T. T. Hou, L. L. Yi, X. L. Yang, J. X. Ke, Y. Hu, Q. Yang, P. Zhou, W. S. Hu, "Maximizing the security of chaotic optical communications," Opt. Express **24**(20), 023439-023449 (2016).