Secure Spread Spectrum Communication Using Super-Orthogonal Optical Chaos Signals

Qing Chen, Yuanyuan Fan, Mengfan Cheng, and Xiaojing Gao

***Abstract*—This paper proposes an analog spread spectrum secure communication system by designing a super-orthogonal two-dimensional electro-optic time delayed chaotic system. Two negatively correlated (called "super-orthogonal") broadband optical chaotic signals can be generated. According to the binary symbol to be transmitted, the two signals are coupled into channel in turn. Benefiting from the wide spectrum and super-orthogonal characteristics of the two optical chaotic signals, the scheme shows excellent anti-noise performance which is verified by numerical simulations. Moreover, by introducing the modulation signal time delay feedback, the security of the system can be improved. The system is capable of resisting time delay signature extraction and return map attack, which are inherent vulnerabilities of time-delayed chaotic system and chaotic shift keying mechanism.**

***Index Terms*—Optical chaos communication, chaotic shift keying, anti-noise performance.**

I. Introduction

FOR secure communications at the physical layer, chaos system has received more and more attention. Chaotic signals generated at the physical layer have significant advantages of noise-like characteristics, unpredictability, high dynamical complexity, and especially remarkable wide-band spectrum [1]–[3]. Encrypting data by using chaotic signals, there are mainly three modulation mechanisms: chaos parameter modulation (CPM), chaos masking (CM), and chaos shift keying (CSK) [4].

The CM communication system has a simple encryption mechanism. Message signal is directly added into the chaotic carrier to produce encrypted signals. In recent years, CM communication has been drawing considerable interest in data secure transmission in optical fiber links [5]. Research topics relates mainly to the data rate and the distance of optical chaos communication. The transmission rate from 2×10Gb/s to 4×12.5 Gb/s are realized in turn, by using wavelength division multiplexing (WDM) technology [2], [6]. Based on advanced modulation format, the spectrum efficiency is improved [7], [8]. Long-haul chaos secure transmission is explored by utilizing coherent detection [3], [9], [10]. However, CM is very sensitive to channel noise [11]. To guarantee message masking and minimize the disturbance of message signal to chaos synchronization at the receiver side, the power of message signal should be particularly weaker than that of chaos carrier [12]. As a result, CM communication can be carried out in the optical fiber link operating at high signal-to-noise ratio, but not be suitable for some practical communication environments, including underwater communication, wireless communication, and free space communication. In these scenarios, worse signal deterioration caused by noise, atmospheric turbulence, or signal attenuation is inevitable.

Among these three mechanisms listed above, CSK can offer the best robustness under non-ideal channels [13], [14]. CSK can be divided into two categories: coherent chaotic shift keying (CCSK) and non-coherent differential CSK (DCSK). In DCSK system, the demodulation is carried out without chaotic carrier reproduction, which means that the parameter sensitivity of chaos system is not used to enable the security of communication system. Therefore, DCSK has good anti-noise performance but at the cost of security degradation [15]. Different from DCSK, in CCSK system, chaotic carriers must be reproduced for message recovery. An eavesdropper cannot recover the message without prior knowledge of the hardware and parameter settings. Therefore, CCSK can provide higher security but lower anti-noise ability. Even so, there still exist possibilities and great significances in improving the anti-noise performance of CCSK for data security transmission in non-ideal channels.

To design CCSK communication systems under strong noise condition, there are two conflicting design requirements (i.e., message confidentiality and reliable message recovery). Based on the channel capacity theory, using optical chaos signals with a wide spectrum of more than ten or even tens of GHz as spread spectrum signal, the energy of signal can be spread over a wide bandwidth to effectively improve the anti-noise tolerance. Now, optical chaos system subjected to all-optical/opto-electronic time-delayed feedback is a major type of optical chaos generator.

Manuscript received May 10, 2022; revised May 31, 2022; accepted June 5, 2022. Date of publication June 10, 2022; date of current version June 20, 2022. This work was supported in part by the National Key Research and Development Program of China under Grant 2021YFB2900901, in part by the National Natural Science Foundation of China under Grant 62175077, in part by the Science and Technology Planning Project of Shenzhen Municipality under Grant JCYJ20200109144012410, in part by the Open Program of the State Key Laboratory of Advanced Optical Communication System and Networks at Shanghai Jiao Tong University, China under Grant 2022GZKF013, and in part by the Teaching Laboratory Open Foundation of China University of Geosciences under Grant SKJ2021214. *(Corresponding author: Xiaojing Gao.)*

Qing Chen and Yuanyuan Fan are with the School of Computer Science, China University of Geosciences, Wuhan 430074, China (e-mail: 1690147840@qq.com; yyfan@cug.edu.cn).

Mengfan Cheng is with the Next Generation Internet Access National Engineering, School of Optical and Electronic Information, Huazhong University of Science and Technology, Wuhan 430074, China, and also with the Research Institute of Huazhong University of Science and Technology in Shenzhen, Shenzhen 518000, China (e-mail: chengmf@mail.hust.edu.cn).

Xiaojing Gao is with the School of Computer Science, China University of Geosciences, Wuhan 430074, China, and also with the State Key Laboratory of Advanced Optical Communication System and Networks, Shanghai Jiao Tong University, Shanghai 200240, China (e-mail: gaoxj@cug.edu.cn).

Digital Object Identifier 10.1109/JPHOT.2022.3181327

The security of such a time delay optical chaos communication system relies mainly on the suppression of time delay parameter (i.e., time delay signature, TDS) [16]–[18]. However, there are several methods succeed in recovering the TDS [19]. Meanwhile the return map attack is a major challenge for traditional CSK communication systems [20], [21]. Moreover, dispreading by monitoring synchronized error is sensitive to noise, which is considered as one practical drawback of the CCSK systems. There are few methods proposed to design an optical CCSK system. In [13], a chaos system with a digital-analog hybrid time delayed feedback structure is proposed. It is no longer suffered from return map attack and TDS extraction and has better anti-noise performance, but the data communication rate seriously decreases. In [22], an optical CCSK communication system is proposed by introducing a novel correlation demodulator. The system can tolerate a higher noise level. However, the chaos synchronization driving signal needs to be sent to the receiver through an optical fiber channel. Moreover, the return map attack is not tested. Thus, when designing an optical CCSK communication system, researchers will meet some problems, i.e., TDS concealment, return map attack, and anti-noise tolerance, which need to be taken into account.

In this paper, a two-dimensional super-orthogonal electro-optic time delay chaos system is constructed as the transmitter. Two "super-orthogonal" optical chaotic signals with a wide frequency spectrum can be generated to bear the information of bits 1 and 0, respectively. At the receiver side, after synchronization occurs, the message is decoded by calculating the correlation between the input and output of the receiver. The orthogonalization of the two optical spread spectrum signals makes the system have better anti-noise performance, as shown in our simulation results. Moreover, different from the traditional CCSK scheme, the modulation signal with time delay is injected into the chaotic system to complicate the nonlinear characteristics of the system. As a result, the system we called quadrature analog spread spectrum (QASS) is resistant to TDS extraction and return map attack. Focusing attention on the problem of strong noise, the proposed system has the potential to be used for secure communication in practical non-ideal communication scenarios.

II. QASS Modulation and Demodulation

The proposed QASS communication system is depicted in Fig. 1. The emitter is composed of two electro-optical (EO) feedback loops. Each loop consists of a laser diode (LD), Mach–Zehnder modulator (MZM), optical delay line (DL), polarization controller (PC), photodetector (PD), and radio-frequency amplifier (RF). In the first branch, the pump current injected into LD1 switches between L_0 and L_1 depending on the binary symbol $m(t) \in \{0,\ 1\}$ to be transmitted. Orthogonally, the pump current injected into LD2 switches between L_0 and L_1 according to the inverted binary symbol $1 - m(t)$. The laser beams emitted from LD1 and LD2 are respectively fed into MZM1 and MZM2 to generate two optical chaos signals $s_1(t)$ and $s_2(t)$. Then, they are coupled and split into three parts. One part is used as the information-bearing waveform to be transmitted for

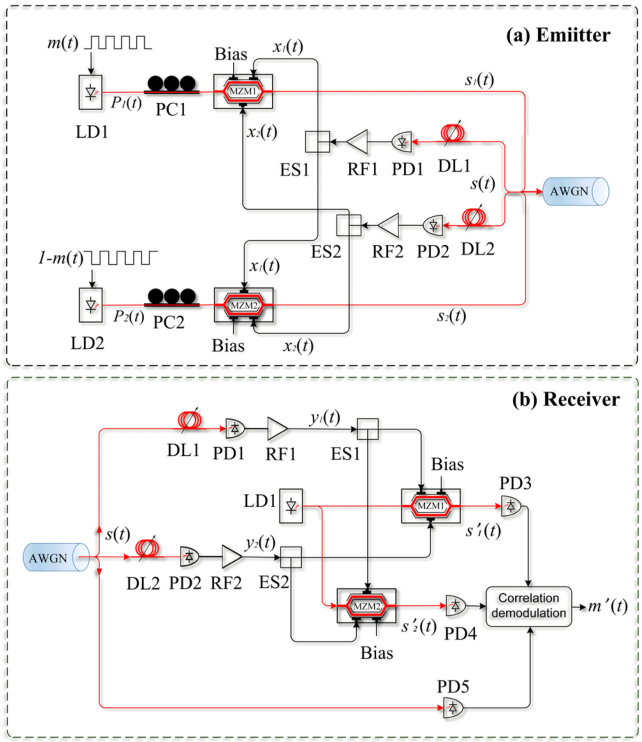

Fig. 1. Simplified block diagram of the QASS communication system.

communication. The other two parts are transmitted through delay lines $\tau_1(t)$ and $\tau_2(t)$ respectively.

Then, the time delayed signals are detected and converted into electric signals by PD1 and PD2. After being amplified by RF1 and RF2, we can obtain two electric outputs represented by $x_1(t)$ and $x_2(t)$. In our scheme, the upper and lower arms of MZM1 are driven by signals $x_1(t)$ and $x_2(t)$ respectively, and those of MZM2 are driven by the same signals in the reverse order. The nonlinear transformation produced by MZMs are expressed as:

$$\begin{cases} s_1(t) = \beta_1 \cos^2\left(x_1(t) - x_2(t) + \varphi_1\right) \\ s_2(t) = \beta_2 \cos^2\left(x_2(t) - x_1(t) + \varphi_2\right) \end{cases} \tag{1}$$

where s_i is the output of MZM$_i$, $\beta_i(t)$ is defined as the nonlinear feedback strength, and φ_i is the offset phase, $i = 1, 2$. The dynamics of the proposed system can be modeled by an electro-optical time delay equation as follows:

$$\begin{cases} \frac{dx_1}{dt} = -x_1 - a\int_0^t x_1(t)\,dt + s_1(t-\tau_1) + s_2(t-\tau_1) \\ \frac{dx_2}{dt} = -x_2 - a\int_0^t x_2(t)\,dt + s_1(t-\tau_2) + s_2(t-\tau_2) \end{cases} \tag{2}$$

where τ_i is the time delay parameter, and a is the response time of the feedback loop. By appropriately setting L_0 and L_1, the powers $P_1(t)$ and $P_2(t)$ of LD1 and LD2 satisfy the following relationship: when binary symbol equals $m(t) = 1$, $P_1(t) \gg P_2(t)$, otherwise $P_1(t) \ll P_2(t)$. In other words, according to the bit to be transmitted in each transmission period, the outputs $s_1(t)$ and $s_2(t)$ are coupled to generate a mixed

signal $s(t)$ expressed as:

$$\begin{cases} s(t) \approx s_1(t), \text{ if } m(t) = 1 \\ s(t) \approx s_2(t), \text{ if } m(t) = 0 \end{cases} \tag{3}$$

Signal $s(t)$ is transmitted to the receiver through an additive white gaussian noise channel, then the captured signal at the receiver end can be obtained as follows

$$\begin{cases} s(t) \approx s_1(t) + n(t), \text{ if } m(t) = 1 \\ s(t) \approx s_2(t) + n(t), \text{ if } m(t) = 0 \end{cases} \tag{4}$$

where $n(t)$ is the additive white Gaussian noise (AWGN).

As shown in Fig. 1(b), received signal $s(t)$ is split into three branches. Two parts are transmitted through delay lines $\tau_1(t)$ and $\tau_2(t)$ respectively to generate time delayed optical beams which are detected and sent to RFs by PDs. Then from RF1 and RF2, we can obtain electric signals $y_1(t)$ and $y_2(t)$ which can be expressed as

$$\begin{cases} \frac{dy_1}{dt} = -y_1 - a\int_0^t y_1(t)\,dt + s(t-\tau_1) \\ \frac{dy_2}{dt} = -y_2 - a\int_0^t y_2(t)\,dt + s(t-\tau_2) \end{cases} \tag{5}$$

At the receiver side, the power of the output light of LD is kept constant. Signals $y_1(t)$ and $y_2(t)$ are sent into MZM1 and MZM2 upside down to drive the arms. Then we can get the reference signals, $s'_1(t)$ and $s'_2(t)$, which are expressed as

$$\begin{cases} s'_1(t) = \beta_1 \cos^2(y_1(t) - y_2(t) + \varphi_1) \\ s'_2(t) = \beta_2 \cos^2(y_2(t) - y_1(t) + \varphi_2) \end{cases} \tag{6}$$

The two reference optical signals and the third optical beam are received by PDs and fed into the correlation demodulation module. In each transmission period, the correlation coefficient between $s(t)$ and $s'_1(t)$ noted by $C_1(t)$ and the correlation coefficient between $s(t)$ and $s'_2(t)$ denoted by $C_1(t)$ are calculated. The correlation coefficient (CC) is defined as [8]:

$$C = \frac{\langle [s(t) - \langle s(t)\rangle][s'_i(t) - \langle s'_i(t)\rangle]\rangle}{\sqrt{\left\langle [s(t) - \langle s(t)\rangle]^2 \right\rangle \left\langle [s'_i(t) - \langle s'_i(t)\rangle]^2 \right\rangle}} \tag{7}$$

where $\langle\cdot\rangle$ stands for the time average. Based on the outputs $C_1(t)$ and $C_2(t)$ of the correlator, a decision about the received symbol is taken, which can be described as

$$\begin{cases} m'(t) = 1, & \text{if } C_1(t) - C_2(t) > 0 \\ m'(t) = 0, & \text{if } C_2(t) - C_1(t) > 0 \end{cases} \tag{8}$$

III. Main Results

The transmitter-receiver setup according to (1)–(8) is numerically carried out by using the toolkit in MATLAB R2018b. The system parameters are set as $a = 3.3 \times 10^{-6}$, $\beta_1 = 5$, $\beta_2 = 4$, $\varphi_1 = \varphi_2 = -\pi/4$, and time delay values are set as $\tau_1 = 20$ ns, $\tau_2 = 30$ ns. Simulation results are shown in Fig. 2. The waveform of the message signal of 1 Gbit/s is shown in Fig. 2(a) while Fig. 2(b) shows the transmitted information-bearing chaotic signal $s(t)$. The power of the binary digital signal is expanded to about 20 GHz bandwidth as shown in Fig. 2(c). It is found that there are no clear signatures in the time and frequency domains. When the SNR is 10 dB, By calculating the correlation comparison (i.e., $C_1 - C_2$) at the receiver side, the error-free decryption can be established as shown in Fig. 2(d). These results show that the communication system has a desirable anti-noise performance.

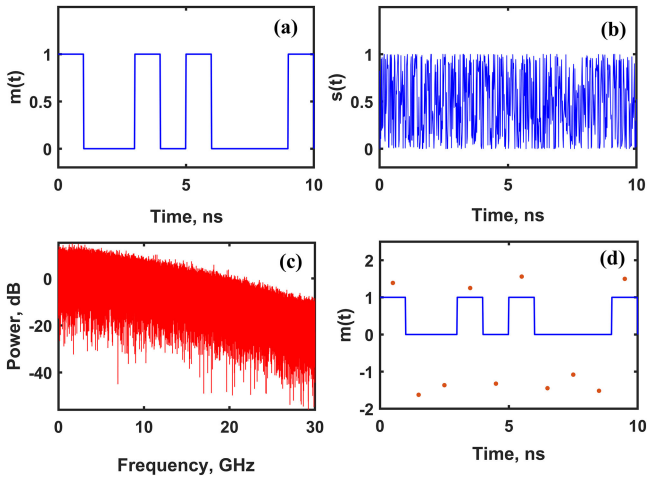

Fig. 2. QASS modulation and demodulation. (a) An example of 1Gbit/s digital message, (b) information-bearing chaotic signal $s(t)$, (c) corresponding spectrum, and (d) message recovery (points show correlation comparison $C_1(t) - C_2(t)$ calculated in bit periods).

IV. Security Analysis

The degree of security of the proposed system is evaluated in detail. We consider two attack scenarios as follows: encryption key i.e., time delay signature (TDS) extraction and decryption of the message by extracting the statistical properties of the ciphertext.

A. Time Delay Concealment

To extract the TDS, a variety of statistical analysis methods have been proposed in the literature [23]–[25], such as auto-correlation function (ACF), delayed mutual information (DMI), permutation-information-theory approach (PE). Among those, ACF and DMI are robust to noise. For a time series $x(t)$, they are defined as follows:

$$C(l) = \frac{\langle [x(t) - \langle x(t)\rangle][x(t-l) - \langle x(t-l)\rangle]\rangle}{\sqrt{[x(t) - \langle x(t)\rangle]^2 \left[x(t-l) - \langle x(t-l)\rangle^2\right]}} \tag{9}$$

and

$$D(l) = \sum P(x(t), x(t-l)) \times \ln \frac{P(x(t), x(t-l))}{P(x(t))\,P(x(t-l))} \tag{10}$$

where $\langle\cdot\rangle$ means the time average, l means the time delay, $P(x(t))$ and $P(x(t-l)$ represent the probability distribution of $x(t)$ and $x(t-l)$ respectively, and $P(x(t), x(t-l))$ is the joint probability distribution of $x(t)$ and $x(t-l)$. The TDS extraction by using ACF and DMI is visualized in Fig. 3(a) and (b). There are no obvious peaks, which means that an eavesdropper cannot

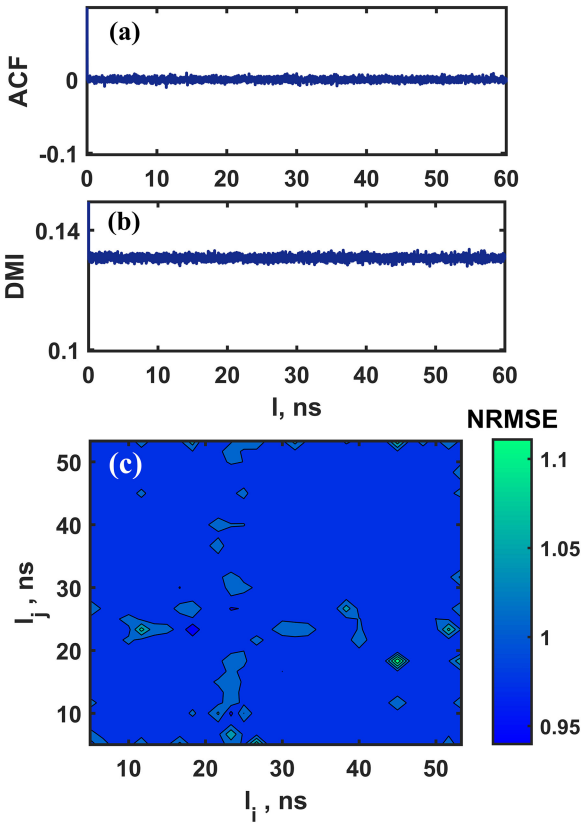

Fig. 3. TDS extraction. (a) The ACF, (b) DMI, (c) the NRMSE function versus l_i and l_k.

extract the TDS by using ACF and DMI calculated from signal $s(t)$. However, having the anti-statistical analysis ability does not mean resistance to reverse model analysis [26]. A TDS extraction method based on deep learning has been proposed recently, which presents new threats to the security of time delay chaos communication systems [26]. A model set $\{\varphi_{ik}\}$ can be obtained by training the relationship between encrypted signal $s(t)$ and its delayed variations $s(t-l_i)$ and $s(t-l_k)$, which is described as the following:

$$\left(s\left(t-l_i\right), s\left(t-l_k\right)\right) \rightarrow s\left(t\right),\ i,k\ =\ 1,\ldots. \tag{11}$$

where (l_i, l_k) are time delay candidates. The prediction ability of φ_{ik} is evaluated by using normalized root mean square error (NRMSE) expressed as [26]:

$$E_{ik} = \frac{\sum_{m=1}^{n}\left(x_m - y_m\right)^2}{\sum_{m=1}^{n}\left(x_m - \bar{x}\right)^2} \tag{12}$$

where x_m is the original sequence, y_m is the predicted sequence, and $\bar{x}$ is the mean value of x. The prediction ability of φ_{ik} is used to identify the TDS [26]. If the TDS can be extracted, the NRMSE function versus (l_i, l_k) will exhibit a peak located at $(\ l_i = \tau_1\ ,\ l_k = \tau_2\ )$. Varying l_i and l_k in the range of $[553.3]$ ns with fixed step size $h\ =\ 1$ ns, we map E_{ik} in $l_i - l_k$ plane, which is plotted in Fig. 3(c). It is found that there is no obvious peak at the sections defined by $l_i =\ 20$ ns and $l_k =\ 30$ ns.

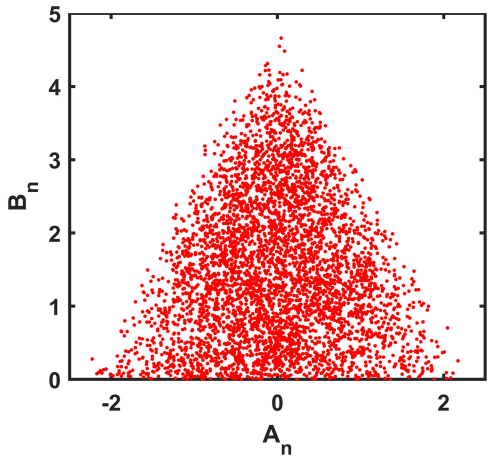

Fig. 4. The return map of system.

These results show that the proposed system can against TDS recovery considering ACF, DMI, and deep-learning-based reverse modeling.

B. Return Map Attack

The encoding process described by (3) is tested by using return map. The return map is usually used to detect the switching perturbation of a chaotic signal, which was proposed in [20], [21]. For a chaotic signal $x(t)$, two variables are defined as follows:

$$\begin{cases} A_n = \left(Q_n + P_n\right)\ /2 \\ B_n = Q_n\ - P_n \end{cases} \tag{13}$$

where Q_n and P_n are the nth maxima and nth minima of the signal. Using signal $s(t)$ from emitter, we plot a return map i.e., A_n vs B_n in Fig. 4. There are no different two strips representing 0-bit or 1-bit, but a diffused pattern. Different from traditional CSK method, in our system, the spread spectrum signals $s_1(t)$ and $s_2(t)$ are generated under the drive of the same signal $s(t)$ just with different time delays τ_1 and τ_2. Therefore, it is easy to control the range of the two signals so that they are not far away. As a result, no significant information can be obtained from the statistical distribution characteristic of maxima and minima points. The proposed system is effective against return-map attack.

V. Transmission Performance

In this Section, the transmission performance of the QASS communication system is analyzed in detail. The bit-error-rate (BER) versus data rate is shown in Fig. 5(a) for different signal-to-noise ratios (SNR). For SNR $=$ 5, 10, 15 dB, it can be observed that the BER performance is getting worse as the bit rate is increased and the SNR is decreased. For data transmission rate up to 2Gbit/s, the SNR should be SNR $\geq$ 10 dB, then error-free transmission can be maintained. When SNR $=$ 10, 15 dB, to achieve BER $\leq 3.8 \times 10^{-3}$, the data rate should be lower than 4Gbit/s, and 6Gbit/s, respectively. Even if the SNR is reduced to 5 dB, data rate can reach 800Mbit/s

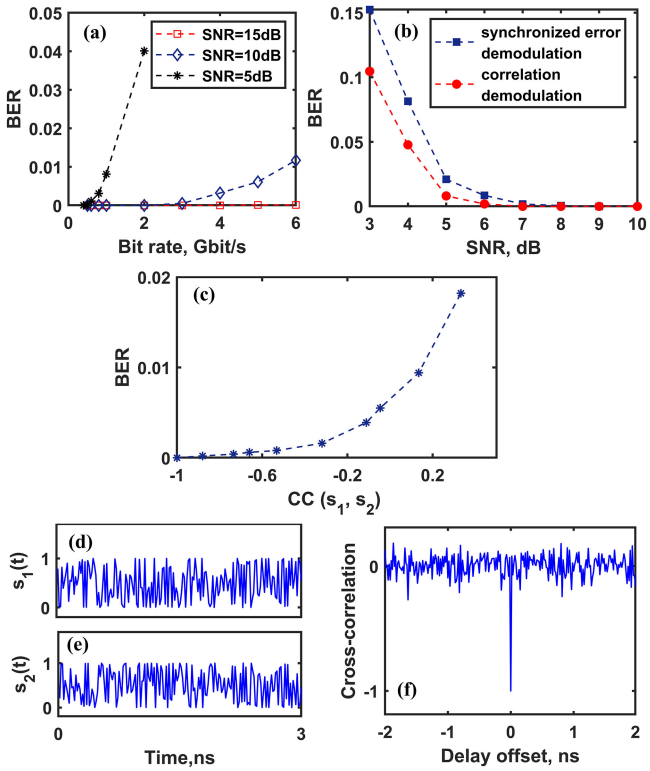

Fig. 5. (a) BER versus data rate for SNR = 5 dB, 10 dB and 15 dB. (b) BER versus SNR for the proposed system by using CC comparison demodulator (●) and synchronization error demodulator (■). (c) BER versus CC, CC = −1, −0.8797, −0.7346, −0.6599, −0.5323, −0.3192, −0.1112, −0.0462, 0.1346, and 0.3325. (d) Time series of s_1 and (e) s_2. (f) The Correlation between $s_1(t)$ and $s_2(t)$.

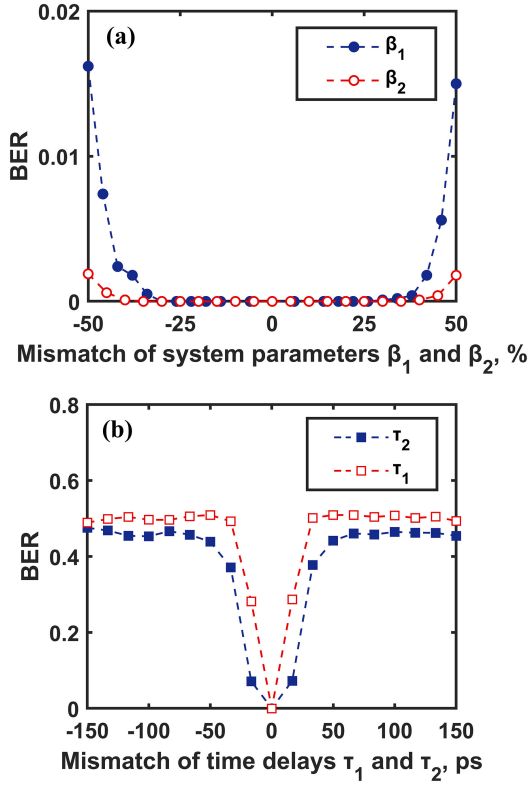

Fig. 6. (a) Influence of system parameter β_1 mismatch (●) and β_2 mismatch (○) on the BER. (b) BER versus time delay τ_1 mismatch (□) and time delay τ_2 mismatch (■).

(BER $= 3.1 \times 10^{-3}$). Moreover, for the conventional CSK system based on synchronization error demodulator and QASS system based on CC comparison, comparison of the BERs versus SNR is shown in Fig. 5(b). It is found that QASS can achieve better BER performance. The reason could be explained as follows. The basic idea underlying the QASS communication system is expanding the bandwidth using optical chaos signals which are orthogonal. The noise tolerance can be improved benefiting from the wide spectrum characteristics of optical chaotic signal. On the other hand, we demodulate the message by using the correlation coefficient (CC), which is described in (7) and (8). The influence of the cross-correlation characteristics of the two information-bearing signals, $s_1(t)$ and $s_2(t)$, on the noise immunity is analyzed in detail. When we set parameters φ_1 and φ_2 as $(-\pi/4, -\pi/4)$, $(-\pi/6, -\pi/4)$, $(-\pi/8, -\pi/4)$, $(-\pi/10, -\pi/4)$, $(-\pi/6, -\pi/6)$, $(-\pi/8, -\pi/6)$, $(-\pi/10, -\pi/6)$, $(-\pi/8, -\pi/8)$, $(-\pi/10, -\pi/8)$, and $(-\pi/10, -\pi/10)$, the corresponding CC is equal to -1, -0.8797, -0.7346, -0.6599, -0.5323, -0.3192, -0.1112, -0.0462, 0.1346, and 0.3325, respectively. When the data rate is 400 Mbit/s and SNR = 5 dB, from Fig. 5(c), we obtain that i) for $CC = -1$, error-free transmission can be obtained; ii) the BER increases with the increasing of CC. These results show that when CC is equal to -1 (i.e., super-orthogonal), the system shows better anti-noise performance. It is worth noting that, 1 and -1 are the maxima and minima extremes of CC. Fig. 5(f) shows CC between signals $s_1(t)$ and $s_2(t)$ plotted in Fig. 5(d) and (e). Their waveforms are reversed, and their cross-correlation coefficient is equal to -1 (i.e., super-orthogonal), which can maximize the anti-noise performance of our system.

VI. Sensitivity of Parameter Mismatch

In a real-world communication environment, the parameters mismatch should be considered. Moreover, from the security point of view, the sensitivity to the encryption key (i.e., TDS) is also a great concern. Therefore, both the robustness and the sensitivity of TDS are discussed. Fig. 6(a) plots the BER performance versus the system parameters β_1 and β_2 mismatches when data rate is set as 4Gbit/s. It is shown that the BER is not highly sensitive to mismatching. The BERs equal 0 when parameter β_1 detuning and parameter β_2 detuning are under 30% and 35%. When the mismatches are under 34% and 40%, BER is less than 6×10^{-4}. Even if the detuning of β_1 grows to 42% and the detuning of β_2 grows to 55%, usable BERs can still be obtained (BER $\leq 3.2 \times 10^{-4}$). The BER versus time delay mismatches is depicted in Fig. 6(b). It is clearly found that the BER performance will degrade seriously even if the time delay mismatch is set at ps level. When the mismatches of time delays τ_1 and τ_2 are both 16.7ps, BER is 0.2816 and 0.0716. For legitimate users, the time delays can be matched accurately by adjusting the length of optical path. Therefore, the QASS scheme is both secure and feasible in real-world applications.

VII. Conclusion

For optical data secure transmission under the condition of low SNR, we proposed an optical CSK communication system called QASS scheme which is derived from the combination of quadrature spread spectrum technique and CSK scheme. It exhibits good BER performance and higher level of security than that of traditional CSK. Simulation results demonstrate that when SNR $\geq$ 10dB, error-free transmission at 2Gbit/s bit rate can be achieved. Even when the SNR is reduced to 5 dB, usable BER $= 3.1 \times 10^{-3}, 1.1 \times 10^{-3}, 6 \times 10^{-4}$ can be obtained for the data rate of 800Mbit/s, 600Mbit/s, 500Mbit/s. Furthermore, neither the TDS extraction nor the return-map attack works on the proposed scheme.

References

[1] A. Zhao, N. Jiang, S. Liu, Y. Zhang, and K. Qiu, "Generation of synchronized wideband complex signals and its application in secure optical communication," *Opt. Exp.*, vol. 28, pp. 23363–23373, Aug. 2020, doi: 10.1364/OE.398119.

[2] A. Zhao, N. Jiang, S. Liu, Y. Zhang, and K. Qiu, "Physical layer encryption for WDM optical communication systems using private chaotic phase scrambling," *J. Lightw. Technol.*, vol. 39, no. 8, pp. 2288–2295, Apr. 2021.

[3] L. Wang *et al.*, "Scheme of coherent optical chaos communication," *Opt. Lett.*, vol. 45, pp. 4762–4765, Sep. 2020, doi: 10.1364/OL.390846.

[4] G. Kaddoum, "Wireless chaos-based communication systems: A comprehensive survey," *IEEE Access*, vol. 4, pp. 2621–2648, 2016, doi: 10.1109/ACCESS.2016.2572730.

[5] J. Ke, L. Yi, G. Xia, and W. Hu, "Chaotic optical communications over 100-km fiber transmission at 30-gb/s bit rate," *Opt. Lett.*, vol. 43, pp. 1323–1326, Mar. 2018, doi: 10.1364/OL.43.001323.

[6] Y. Fu *et al.*, "High-speed optical secure communication with an external noise source and an internal time-delayed feedback loop," *Photon. Res.*, vol. 7, pp. 1306–1313, Nov. 2019, doi: 10.1364/PRJ.7.001306.

[7] J. Ai, L. Wang, and J. Wang, "Secure communications of cap-4 and ook signals over mmf based on electro-optic chaos," *Opt. Lett.*, vol. 42, pp. 3662–3665, Sep. 2017, doi: 10.1364/OL.42.003662.

[8] J. Ke *et al.*, "32gb/s chaotic optical communications by deep-learning-based chaos synchronization," *Opt. Lett.*, vol. 44, pp. 5776–5779, Dec. 2019, doi: 10.1364/OL.44.005776.

[9] Y. Fu *et al.*, "Analog-digital hybrid chaos-based long-haul coherent optical secure communication," *Opt. Lett.*, vol. 46, pp. 1506–1509, 2021.

[10] Z. Yang, L. Yi, J. Ke, Q. Zhuge, Y. Yang, and W. Hu, "Chaotic optical communication over 1000 km transmission by coherent detection," *J. Lightw. Technol.*, vol. 38, no. 17, pp. 4648–4655, Sep. 2020, doi: 10.1109/JLT.2020.2994155.

[11] T. Yang, "A survey of chaotic secure communication systems," *Int. J. Comput. Cogn.*, vol. 2, pp. 81–130, Jun. 2004.

[12] D. A. Mazhar, S. Z. A. Shah, M. K. Islam, and F. Qamar, "Design issues of digital and analog chaotic rof link using chaos message masking," *IEEE Access*, vol. 7, pp. 174042–174050, 2019.

[13] X. Gao, M. Cheng, L. Deng, M. Zhang, S. Fu, and D. Liu, "Robust chaotic-shift-keying scheme based on electro-optical hybrid feedback system," *Opt. Exp.*, vol. 28, pp. 10847–10858, Apr. 2020, doi: 10.1364/OE.389251.

[14] X. Gao, F. Xie, and H. Hu, "Enhancing the security of electro-optic delayed chaotic system with intermittent time-delay modulation and digital chaos," *Opt. Commun.*, vol. 352, pp. 77–83, 2015.

[15] Y. Fang, G. Han, P. Chen, F. C. M. Lau, G. Chen, and L. Wang, "A survey on DCSK-based communication systems and their application to uwb scenarios," *IEEE Commun. Surv. Tut.*, vol. 18, no. 3, pp. 1804–1837, Jul.–Sep. 2016, doi: 10.1109/COMST.2016.2547458.

[16] S. -S. Li *et al.*, "Band-rejection feedback for chaotic time-delay signature suppression in a semiconductor laser," *IEEE Photon. J.*, vol. 14, no. 2, Apr. 2022, Art. no. 1517208, doi: 10.1109/JPHOT.2022.3153640.

[17] N. Jiang, A. Zhao, S. Liu, C. Xue, B. Wang, and K. Qiu, "Generation of broadband chaos with perfect time delay signature suppression by using self-phase-modulated feedback and a microsphere resonator," *Opt. Lett.*, vol. 43, pp. 5359–5362, Oct. 2018.

[18] A. Zhao, N. Jiang, S. Liu, C. Xue, J. Tang, and K. Qiu, "Wideband complex-enhanced chaos generation using a semiconductor laser subject to delay-interfered self-phase-modulated feedback," *Opt. Exp.*, vol. 27, pp. 12336–12348, Apr. 2019.

[19] N. Jiang *et al.*, "Simultaneous bandwidth-enhanced and time delay signature-suppressed chaos generation in semiconductor laser subject to feedback from parallel coupling ring resonators," *Opt. Exp.*, vol. 28, pp. 1999–2009, Jan. 2020.

[20] S. Li, G. Chen, and G. Álvarez, "Return-map cryptanalysis revisited," *Int. J. Bifurcation Chaos*, vol. 16, pp. 1557–1568, 2006, doi: 10.1142/S0218127406015507.

[21] T. Yang, L.-B. Yang, and C.-M. Yang, "Cryptanalyzing chaotic secure communications using return maps," *Phys. Lett. A*, vol. 245, pp. 495–510, Aug. 1998.

[22] Y. Tang, Q. Li, W. Dong, M. Hu, and R. Zeng, "Optical chaotic communication using correlation demodulation between two synchronized chaos lasers," *Opt. Commun.*, vol. 498, Nov. 2021, Art. no. 127232.

[23] D. Rontani, A. Locquet, M. Sciamanna, and D. S. Citrin, and S. Ortin, "Time-delay identification in a chaotic semiconductor laser with optical feedback: A dynamical point of view," *IEEE J. Quantum Electron.*, vol. 45, no. 7, pp. 879–1891, Jul. 2009, doi: 10.1109/JQE.2009.2013116.

[24] L. Zunino, M. C. Soriano, I. Fischer, O. A. Rosso, and C. R. Mirasso, "Permutation-information-theory approach to unveil delay dynamics from time-series analysis," *Phys. Rev. E.*, vol. 82, Oct. 2010, Art. no. 046212, doi: 10.1103/PhysRevE.82.046212.

[25] M. C. Soriano, L. Zunino, O. A. Rosso, I. Fischer, and C. R. Mirasso, "Time scales of a chaotic semiconductor laser with optical feedback under the lens of a permutation information analysis," *IEEE J. Quantum Electron.*, vol. 47, no. 2, pp. 252–261, Feb. 2011, doi: 10.1109/JQE.2010.2078799.

[26] X. Gao *et al.*, "Time delay estimation from the time series for optical chaos systems using deep learning," *Opt. Exp.*, vol. 29, pp. 7904–7915, 2021.