Time-Delay Signature Concealment in a Security-Enhanced Optical System With Dual-Loop Electro-Optic Self-Feedback Phase Encryption

Bin Tang, Xulin Gao, Biao Su, Yuehua An, Anbang Wang, Yuncai Wang, Yuwen Qin, and Zhensen Gao

***Abstract*—In this paper, a novel phase encryption scheme based on a dual-loop electro-optic self-feedback structure is proposed for time-delay signature (TDS) concealment. As for a conventional single-loop feedback structure, the TDS is extremely vulnerable to exposure in the common link, resulting in a fatal weakness in the entire security system, whereas, the introduction of an additional feedback branch, brings about the mutual dynamics between the phase feedbacks, and effectively solves the problem. The modulation depth and dispersion values, which are two crucial variables affecting TDS concealment, are investigated in detail. In principle, the scheme is verified to have better robustness, more security, and can supply large key space. Error-free transmission of high-speed signals is possible. Thanks to the aforementioned benefits, the dual-loop electro-optic structure proposed could inspire fresh ideas for secure optical communication systems in the future.**

***Index Terms*—Secure optical communication, optical phase modulation, electro-optic feedback, TDS concealment.**

I. Introduction

OVER the years, the explosion of data transactions among optical networks poses increasing demands for confidential data security. As the first and firmest natural barrier, the physical layer should be essentially enhanced to provide high-level protection for the entire network [1], [2], [3], [4]. And in the meantime, chaotic communication has attracted a considerable amount of attention from scholars in the field of secure optical communication, owing to its favorable advantages such as strong robustness and high security in the physical layer [5].

In 1990, chaos synchronization was proposed and proved by Pecora and Carroll for the first time [6]. As the key technology of chaotic communication, the mechanism of chaos synchronization arouses much enthusiasm from scholars. In 2005, Argyris et al. successfully achieved the first secure transmission of optical chaos over 100 km, laying a solid foundation for the application of chaos to communication [7]. In 2010, Roman Lavrov implemented differential-phase-shift-keying (DPSK) signal transmission at a rate of 10 Gbps based on the electro-optic feedback chaos [8]. Wang et al. proposed an all-optical chaotic bidirectional secure communication system [9]. Jiang et al. proposed a physically secure enhanced all-optical chaotic communication scheme [2]. Yi et al. successfully implemented a neural network-based approach for chaotic secure communication of higher-order signals [10]. We experimentally demonstrated a pure hardware optical communication scheme based on temporal spreading and self-feedback phase encryption [11]. These emerging results show chaos, implementing in encryption technique, has a promising future in communication security.

Currently, there are two main categories of chaos-based optical signal generation techniques. The first one, known as all-optical chaos, re-inputs the output optical signal into the laser, causing rapid and intricate perturbation of the internal light field to produce chaotic signals. All-optical chaos, however, is more difficult to synchronize well between transceivers due to its higher demands [12]. Furthermore, the influence of relaxation oscillators also limits the chaotic output bandwidth [13], [14], [15]. The other one named the electro-optic feedback modulation method, under the spotlight, is a much more encouraging way to generate ultra-high bandwidth chaos with a flat spectrum. Compared to all-optical chaos, the electro-optic method-generated version has higher robustness, easier synchronization, and greater compatibility with existing commercial networks

Manuscript received 6 December 2022; revised 19 January 2023; accepted 24 January 2023. Date of publication 27 January 2023; date of current version 6 February 2023. This work was supported in part by the National Key R&D Program of China under Grant 2018YFB1801301, in part by the National Natural Science Foundation of China under Grants U22A2087, 61731014, U2001601, 11904057, and 62004047, in part by the Basic and applied basic research project of Guangzhou Basic Research Program under Grant 202102020506, in part by the Research and Development Plan in Key Areas of Guangdong Province under Grant 2018B010114002, and in part by the Guangdong Introducing Innovative and Entrepreneurial Teams of The Pearl River Talent Recruitment Program under Grant 2019ZT08X340. *(Corresponding author: Zhensen Gao.)*

Bin Tang, Xulin Gao, Biao Su, Anbang Wang, and Yuwen Qin are with the Advanced Institute of Photonics, School of Information Engineering, Guangdong University of Technology, Guangzhou 510006, China, and also with the Guangdong Provincial Key Laboratory of Photonics Information Technology, Guangzhou 510006, China (e-mail: 2112003168@mail2.gdut.edu.cn; 2112103031@mail2.gdut.edu.cn; 2112103090@mail2.gdut.edu.cn; wanganbang@tyut.edu.cn; qinyw@gdut.edu.cn).

Yuehua An is with the School of Optoelectronic Engineering, Guangdong Polytechnic Normal University, Guangzhou 510665, China (e-mail: anyuehua@tyut.edu.cn).

Yuncai Wang and Zhensen Gao are with the Advanced Institute of Photonics, School of Information Engineering, Guangdong University of Technology, Guangzhou 510006, China, also with the Guangdong Provincial Key Laboratory of Photonics Information Technology, Guangzhou 510006, China, and also with the Pengcheng Laboratory, Shenzhen 518052, China (e-mail: wangyc@gdut.edu.cn; gaozhensen@gdut.edu.cn).

Digital Object Identifier 10.1109/JPHOT.2023.3240229

[16], [17], [18]. However, the conventional single-loop electro-optic feedback structure suffers from security vulnerabilities such as unavoidable time-delay leakage and limited key space. Since the amplitude or phase of the output can manifest the time that the feedback path has experienced, the autocorrelation function (ACF) and other methods can be used to extract the TDS of the electro-optic feedback system. Moreover, for the reason of the simple structure, the hardware parameters of the traditional electro-optic chaotic sources are very limited, let alone secure against violent cracking by eavesdroppers.

There have been many innovative solutions proposed for TDS concealment. In 2011, Romain et al. experimentally demonstrated that integrating a digital key in the phase-chaotic electro-optic delay system can realize TDS concealment [19]. Gao et al. proposed an electro-optic time-delay chaotic system with an intermittent time-delay modulation strategy [20]. In 2017, Liu et al. provided a three-phase modulated coupling method to achieve TDS cancellation [21]. Two years later, an ingenious time-delay concealment scheme was further proposed, by disturbing the phase correlation with an external noise source, successfully achieving 10 Gbps secure transmission [22]. Wang et al. introduced a scheme involving non-linear coupling of two delayed interfering branches [23]. In 2022, Cheng et al. reported the conception of increasing the nonlinear dimensionality of the chaotic system in the transmitter while decreasing the dimensionality of the transmitted signal [24]. More recently, TDS elimination with enhanced nonlinearity by deep learning has been inventively conceived and demonstrated [25].

To eliminate the TDS, the relevance hiding behind the feedback information should be as much as possibly destroyed, as we can see in all the schemes mentioned above. The time-delay leakage is well suppressed but under the cost of stringent criteria for devices or the extreme complexity of systems. In such cases, a more robust and secured TDS concealment scheme with a concise and practical structure is highly expected.

In this paper, we proposed a novel phase encryption scheme based on the dual-loop electro-optic self-feedback structure for TDS concealment. Due to the use of the dual-loop electro-optic structure, more key parameters are available for encryption, vastly increasing the system security compared to the conventional single-loop structure. Since the confidential data in this scheme is phase encrypted twice at the transmitter side, an eavesdropper cannot simply compensate the encrypted phase and recover the data by just using a conventional single-loop structure to perform malicious attack. In addition, the dual-loop structure makes the feedback signals coupled with each other, which greatly suppresses the autocorrelation and achieves time-delay concealment effectively. Simulation results show that all TDS can be hidden in the ACF at a relatively low modulation depth. This paper is organized into four sections. In Section II, the transmitter and receiver optical paths of the system are introduced, and the dynamic equations of the dual-loop electro-optic self-feedback structure and the functions of each device are described. In Section III, the effect of different parameters on TDS concealment is thoroughly covered, as well as the effectiveness of encryption and decryption in communication and the range of hardware parameter mismatches in the system. Through the above research, the proposed scheme can be perfectly compatible with commercial fiber optic components, and its dual-loop electro-optic structure provides great potential for future physical layer secure optical communication systems.

II. Principle and System Setup

The proposed secure optical communication scheme diagram is divided into three parts: the transmitter side, the transmission link, and the receiver side, as shown in Fig. 1. At the transmitter side, D_1 and D_2 are standard single-mode fibers (SSMF) used as dispersion modules, the primary purpose is to encrypt messages. A 28 Gbps non-return-to-zero (NRZ) signal is modulated in continuous light using a Mach-Zehnder (MZM) optical intensity modulator (IM), and the original message is subsequently scrambled by a dispersion module D_1 with a dispersion value of $\sim$720 ps/nm. After the dispersion, the time domain signal will be reflected as waveform stretching and spectral spreading under the effect of chromatic dispersion, thereby, randomly like a noise. The fluctuation of the noise-like signal, as the modulator driver, is fed into the phase modulator successively through two different branches (PM_1 and PM_2). More specifically, the output of PM_2 is split by a fiber coupler into two parts, one is for transmission, and the other is further divided into two branches, each constructed by a tunable delay line (TDL) and a photodiode (PD) followed by a variable electrical attenuator (VEA) to adjust the feedback strength into the two PMs respectively. In our scheme, TDL_1 is set at 25 ns (T_1), and TDL_2 is set at 15 ns (T_2). The split ratio of the fiber couplers is set as 50:50 for simplicity and there is no special requirement for the split ratio. The structure with double feedback makes the internal phase information interact with each other and reduces the correlation in the phase domain, which can effectively weaken TDS. The dynamics equation of the system can be given by the Ikeda equation as [26]:

$$x_i(t) + \tau_i \frac{dx_i(t)}{dt} + \frac{1}{\theta_i}\int_{t_n}^{t} x_i(s)ds = \beta_i \cos^2[x_i(t - T_i)] \quad (1)$$

where $\beta_i = P_0\ G\eta A\pi/(2V_\pi)$, $(i = 1, 2)$, is the overall gain in the loop, in which G is the electrically amplified gain, P_0 is the input optical power, A is the total attenuation, V_π is the modulated half-wave voltage, and η with respect to the sensitivity of the PD. Furthermore, τ and θ are the differential and integral response times, concerning the high and low cut-off frequency of the bandpass filter, respectively. The transformation of phase modulation to intensity modulation (PM-to-IM) is accomplished by a dispersion module D_2 with a value of approximately 1200 ps/nm. Since the transmitter is a physical layer encryption module consisting of pure hardware parameters, the parameters of each device can be used as considerable and credible keys, and therefore, provide a satisfactorily large key space.

Information recovery is achieved by using an open-loop structure with highly matched parameters to the transmitter side. Firstly, the encrypted signal passed through the D_3 with the value of -1200 ps/nm, aiming to recover the dispersion disturbance of D_2. Then, it is divided into two parts by FC_3 (50/50), one is used as a carrier through PM_3 and PM_4. The

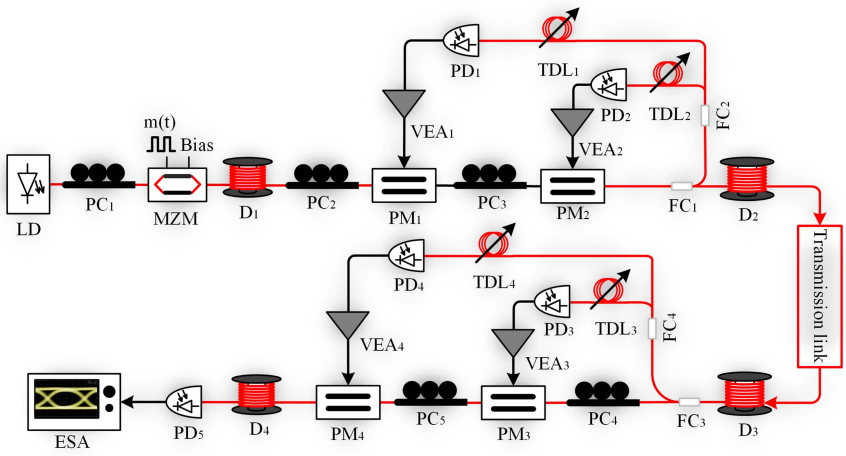

Fig. 1. Experimental setup of the secure communication system: LD, laser diode; PC, polarization controller; MZM, Mach-Zehnder modulator; D, dispersion module; PM, phase modulator; FC, fiber coupler; TDL, tunable delay line; PD, photodetector; VEA, variable electrical attenuator; ESA, electrical spectrum analyzer.

other is divided into two branches by FC_4 (50/50), both are used as the driving signals after the TDL, PD, and VEA in turn, where the parameter of TDL_3 (T_3) is equal to that of TDL_2, and the same between TDL_4 (T_4) and TDL_1, moreover, the modulation depth of PM_3 is equal to PM_2, and PM_4 is equal to PM_1. Ultimately the output of PM_4 is restored to the original message after D_4 with the value of -720 ps/nm, where D_3 and D_4 are dispersion-compensated fibers (DCF). The role of the legitimate receiver is dispersion compensation, phase recovery, and signal detection in succession. In the process of demodulating, the order of the optical path cannot be changed; it must primely pass D_3 to offset the dispersion damage of D_2, then perform phase recovery, and finally through D_4 to compensate for the dispersion damage of D_1. Even with a proper parameter match, if the decryption order is incorrect, the original message will not be received as intended.

III. Simulation Results

Suppression of TDS is essential to ensure the security of communication in electro-optic feedback structures. The TDS can be extracted using a variety of methods, while ACF is one of the most commonly used. The ACF can be defined as [27]:

$$ACF(s) = \frac{\langle [x(t+s) - \langle x(t) \rangle][x(t) - \langle x(t) \rangle] \rangle}{\sqrt{\langle (x(t) - \langle x(t) \rangle)^2 \rangle \langle (x(t+s) - \langle x(t) \rangle)^2 \rangle}} \quad (2)$$

where s represents the time-shift, $<\cdot>$ means the time-average operation, and $x(t)$ represents the 200 ns time series signal obtained from the transmission link. We use the maximum value of the absolute ACF to represent the ACF peak at TDS. By autocorrelating the timing signal, we observed the TDS to determine whether the time delay is concealed. To further quantify the TDS concealment performance, we investigated the relationship between the background Q and TDS, where Q stands for the maximum absolute ACF value for the background autocorrelation signal and it can be determined by the value of Q_f. If the absolute value of ACF is smaller than the background Q, it indicates that the TDS is successfully concealed. The calculation of the background Q can be obtained as follows [9]:

$$\begin{aligned} Q_f(\Delta) &= \left[\underline{P_f}(\Delta), \overline{P_f}(\Delta)\right] \\ \underline{P_f}(\Delta) &= mean\{f(x_\Delta)\} - SD\{f(x_\Delta)\} \\ \overline{P_f}(\Delta) &= mean\{f(x_\Delta)\} + SD\{f(x_\Delta)\} \end{aligned} \quad (3)$$

where Δ indicates the modulation depth or dispersion value, $\underline{Q_f}$ denotes the background ACF measured under different variables, SD is the standard deviation and f represents the ACF function.

A. Relationship Between Modulation Depth and TDS

To ensure the validity of the phase modulator during encryption, we analyzed the minimum modulation depth range required for PM_1 (β_1) and PM_2 (β_2). Phase encryption will be ineffective if the modulation depth is too small, which makes the structure insufficient to guarantee information security. By intercepting the encrypted signal in the transmission link and compensating for all dispersion impairments but without phase recovery, we determined the minimum effective modulation depth by the eavesdropped bit-error-rate (BER), as shown in Fig. 2. Due to the absence of any phase recovery, the eavesdropper measured BER above the 7% hard-decision forward error correction (HD-FEC) limit of 3.8×10^{-3}, as in the area pointed by the arrow, indicating the phase modulator is functioning. It is recommended that the modulation depth in the scheme be greater than 0.5 to ensure the secure and reliable communication of the system.

Afterward, we numerically simulated the influence of β_1 and β_2 on TDS and plotted the relationship when the dispersion of D_1 is $\sim$720 ps/nm and the dispersion of D_2 is $\sim$1200 ps/nm respectively, as shown in Fig. 3(a) and (b). We imitated an eavesdropper to intercept the encrypted data of the transmission link and determined whether the system successfully concealed the TDS. Meanwhile, by measuring the background Q values

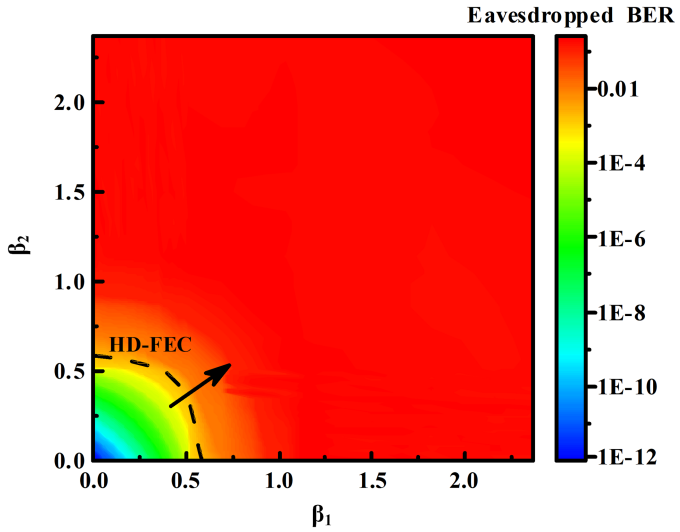

Fig. 2. Two-dimensional map of modulation depth β_1 and modulation depth β_2 variations on eavesdropped BER.

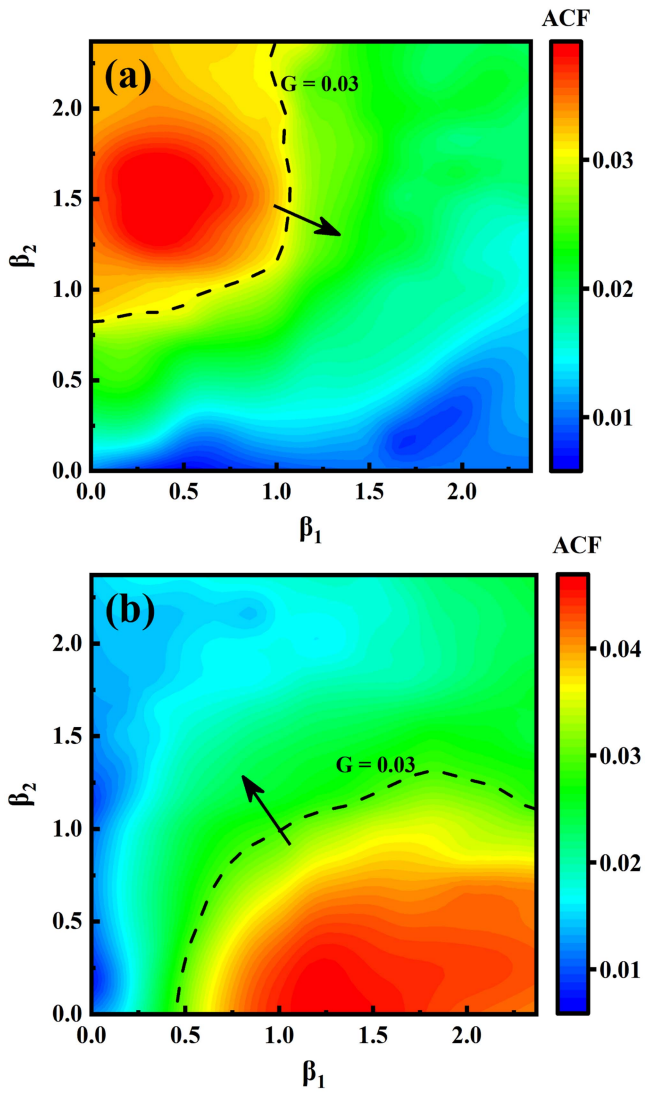

Fig. 3. The two-dimensional map of ACF versus β_1 and β_2: (a) discussion of TDS concealment at T_2; (b) discussion of TDS concealment at T_1.

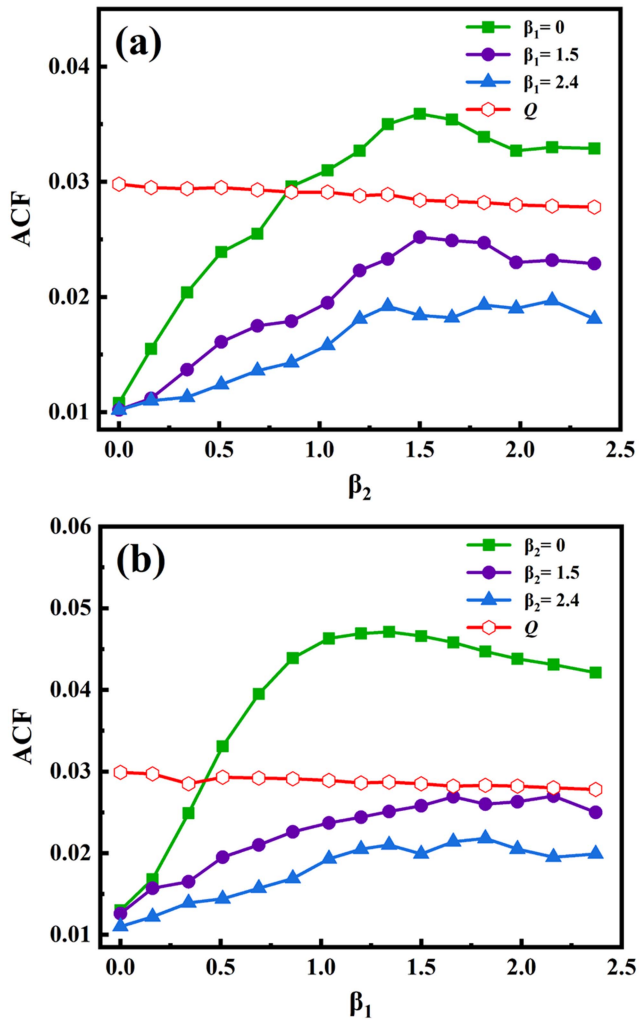

Fig. 4. The relationship between (a) β_2 versus ACF at T_2 and (b) β_1 versus ACF at T_1.

at different modulation depths, we find the Q values are around 0.03. The arrow-pointed interval denotes the peak ACF is smaller than the background Q. In Fig. 3(a), it can be intuitively observed that the regions where the ACF is higher than Q are closer to the vertical axis (β_2), this is because the feedback loop of PM_2 constitutes a time delay of T_2, resulting in a significantly greater impact of β_2 on T_2. As β_1 gradually increases, the ACF of T_2 is gradually lower than the background Q. The reason behind this is the interaction of the phase information between the two branches, which attenuates the TDS. Fig. 3(b), shows the effect of modulation depth on T_1. Similar to T_2, when β_2 is small, the region where ACF is greater than Q will be closer to the horizontal axis (β_1) because of the dominant influence of β_1 on T_1. With the increase of β_2, the ACF of T_1 will likewise become weaker. To achieve better TDS concealment in T_1 and T_2, both β_1 and β_2 should preferably be greater than 1.5, which is smaller than most schemes.

Fig. 4(a) and (b) shows the effects on the ACF with only one feedback branch and with two. As can be seen from Fig. 4(a), when $\beta_1 = 0$, the system structure is analog to one feedback,

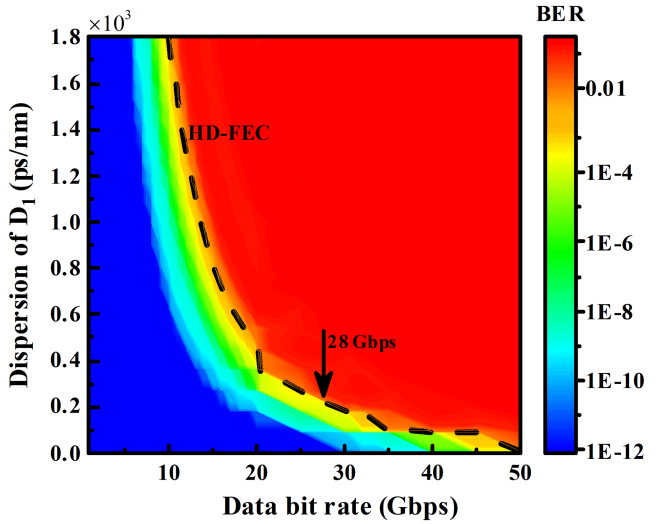

Fig. 5. The two-dimensional map of BER versus data bit rate and dispersion of D_1.

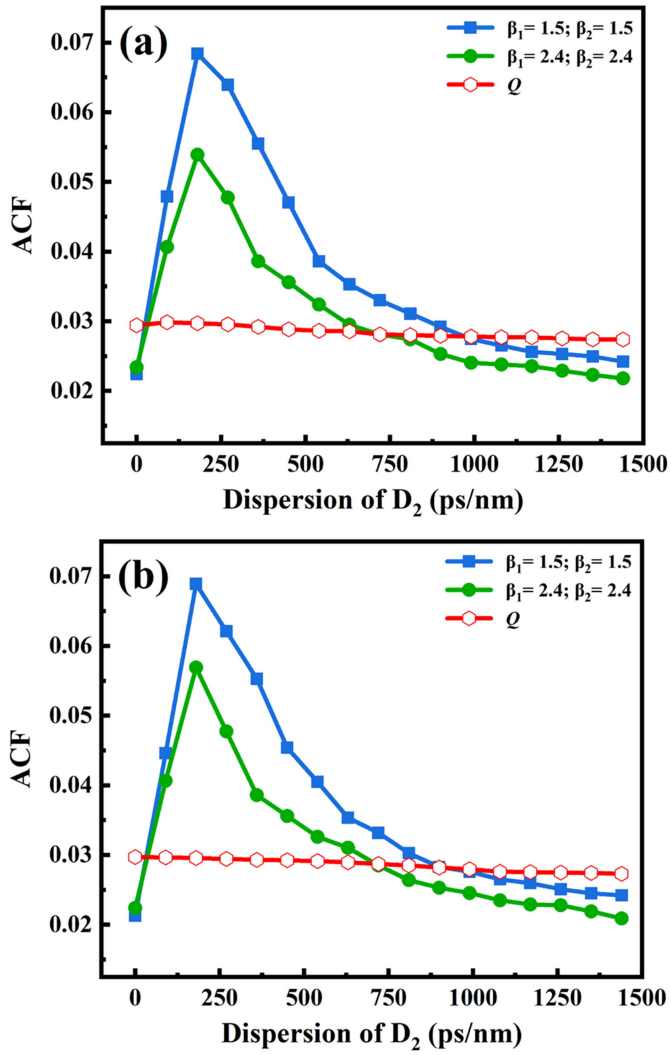

Fig. 6. The relationship between the dispersion of D_2 and ACF (a) at T_1 and (b) at T_2.

under the condition that β_2 is greater than 0.75, the ACF at T_2 is all above Q, which implies TDS is at risk of being intercepted. With the increase of β_1, the system is analogously turned into a double feedback structure, the ACF gradually decreases to be lower than the background overall, confirming the introduction of β_1 has a significant effect on weakening the TDS at T_2. A similar conclusion can be drawn from Fig. 4(b). In the absence of β_2, T_1 is overall exposed, but ACF decreases as β_2 increases, implying a significant influence on T_1 by the introduction of β_2 as well. Consequently, we can conclude that the introduction of an additional feedback branch, on the one hand, effectively suppresses the TDS, so that the eavesdropper has virtually impossible to obtain the delay parameters of the transmission link and the system security is surely guaranteed. On the other hand, more key parameters are available, which greatly enhances the key space of the communication system and ensures resistance from being violently cracked by eavesdroppers.

B. Relationship Between Dispersion and TDS

In our scheme, the dispersion, producing the conversion between phase and intensity, deem to be significantly indispensable for the progress of encryption and decryption. So, the detailed discussions in selecting the dispersion are given below. D_1 scrambles the original message after it is generated, turning it into a noise-like signal. With D_1 values not sufficient to distort the sequence, the drive signal fed back to the phase modulator through the dual-loop structure will not cause such confusion for encryption. We use the BER of the signal after the scrambling of D_1 to evaluate the extent of disorganization, then select an appropriate value for dispersion. As shown in Fig. 5, for the same extent of the BER, the higher the signal speed, the lower the D_1 value needed. In the numerical simulation, we used a 28 Gbps NRZ signal and the dispersion value of D_1 should be at least ~300 ps/nm greater than the value indicated by the arrow to satisfy the information disruption requirement. Therefore, we set D_1 to ~720 ps/nm for a better performance of the encryption.

Then the relationship between the value of D_2 and TDS is further investigated when D_1 is set at 720 ps/nm. Furthermore, to illustrate how varied modulation depths impact the concealment effect more clearly, we addressed the situation of two distinct modulation depths ($\beta_1 = \beta_2 = 1.5$ and $\beta_1 = \beta_2 = 2.4$), as shown in Fig. 6(a) and (b). The trend of the curve shows that both peaks are increasing during the change of D_2 from 0 to 250 ps/nm. This is because the measured ACF will show an increasing trend since more phase information is converted into the intensity domain. When the D_2 is greater than 250 ps/nm, the excessive dispersion value will also take a scrambling effect, which will somehow make the sequence correlation decrease and thus will also lead to a gradual decrease in the ACF. When $\beta_1 = \beta_2 = 1.5$, the dispersion required for D_2 to fully conceal the TDS should be greater than 1000 ps/nm. Yet, with both modulation depths increasing to 2.4, the required dispersion decreases, necessitating about 800 ps/nm. It means the increment of the modulation depth lessens the reliance on dispersion and reduces the device requirements, however, if the modulation

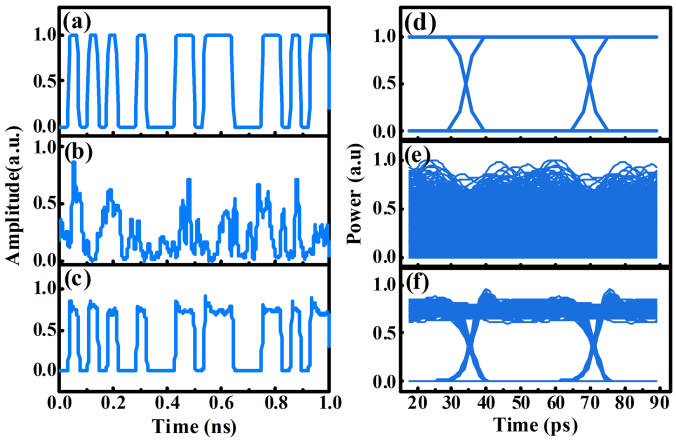

Fig. 7. (a) The waveform at the output of MZM; (b) the waveform at the output of D_2; (c) the waveform at the output of D_4; (d) the eye diagram at the output of MZM; (e) the eye diagram at the output of D_2; (f) the eye diagram at the output of D_4.

depth is too large, the hardware parameter requirement on the legitimate receiver will be more rigorous, which we will discuss in Part C. According to the preceding analysis, we set the value of D_2 as ∼1200 ps/nm.

C. System Performance Analysis

Following the discussion on the selection of hardware characteristics for the solution, the overall performance of the system is investigated and evaluated. First, we plotted the signal waveforms and eye diagrams in different scenarios, which help us visualize signal changes. Then, the two critical evaluation criteria we considered were TDS concealment and system hardware mismatch range. On the one hand, a reliable secure communication system based on electro-optic feedback encryption should provide such assurance that keeps it away from the eavesdropping of its time-delay parameters in the common link, for the dynamic can be easily reconstructed to build a pseudo-legal receiver, posing a serious threat to the security of the system. On the other hand, the practicability of the system should also be thoroughly considered in balance of security and robustness. Strictly-matched hardware parameters between transceivers may bring about superb synchronization for decryption, whereas, it is hard to find such precisely-matched parameters in commercial devices. So, here we investigate the BER performance as the hardware parameter mismatch slightly happens with the premise of ensuring security, to obtain the mismatch range of these parameters. Likewise, to better represent the effect of different modulation depths, we select two cases where the modulation depth can satisfy the delay concealment according to the discussion in Part B, and measure the parameter mismatch range under two different modulation depths.

As the hardware parameters are properly settled and the security demand is well satisfied, we test the communication performance. The corresponding waveforms and eye diagrams are drawn by collecting the timing signals from the transmitter, the transmission link, and the receiver, respectively, to determine

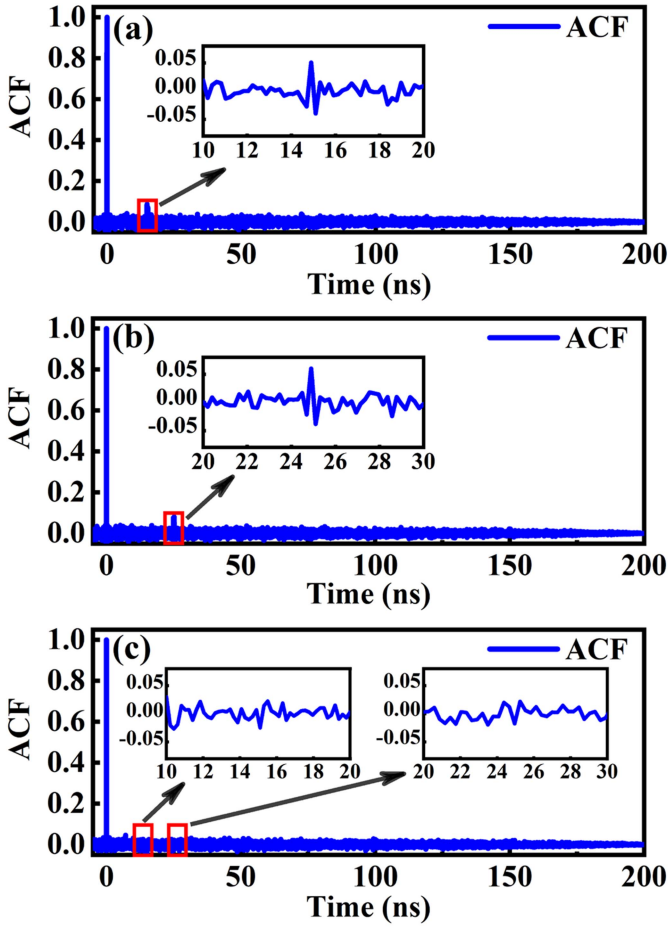

Fig. 8. (a) ACF curves at T_1 ($\beta_1 = 0$, $\beta_2 = 2.4$); (b) ACF curves at T_2 ($\beta_1 = 2.4$, $\beta_2 = 0$); (c) ACF curves with TDS concealment at T_1 and T_2 ($\beta_1 = 2.4$, $\beta_2 = 2.4$).

whether the system can achieve the functions of encryption and decryption in the time domain. As shown in Fig. 7(a)–(c), it can be seen that the original message is a standard NRZ signal with a rate of 28 Gbps. The timing sequence of the transmission link appears out of order after encryption, and the waveform can be restored to the original message only after proper decryption by the legitimate receiver. By comparing the eye diagrams in Fig. 7(d)–(f), we can fully confirm the security assurance of the system for communication. As the eye diagram in the transmission link is completely closed, the eavesdropper cannot use DLF to gather the pertinent information.

Fig. 8(a) and (b) depicted the ACF of the signal intercepted from the transmission common link. In the case of only one feedback loop being active, as in the conventional single-loop feedback structure, we can see there are clear peaks at T_1 and T_2. However, as we learned in our exploration in Part B when an additional feedback branch is introduced within the suitable system parameters, the significant TDS gradually diminishes and eventually becomes as small as the background, demonstrating the time-delay information is concealed. It is strongly verified in Fig. 8(c), where the TDS amplitudes of T_1 and T_2 are similar to the surrounding jitter and are essentially undetectable.

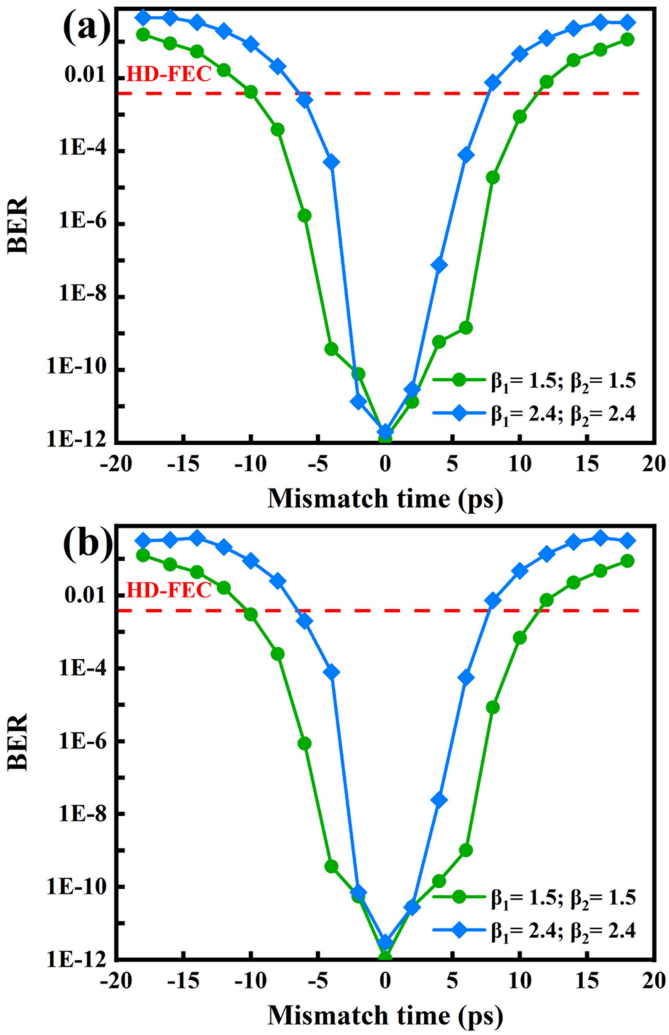

Fig. 9. The time-delay mismatch versus BER (a) at T_1 and (b) at T_2.

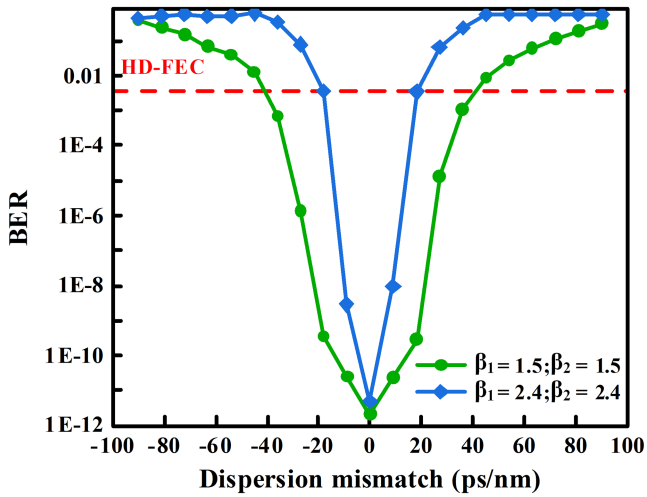

Fig. 10. The dispersion value mismatch of D_2 versus BER.

This indicates the entire delay peaks can be suppressed by our suggested structure, further enhancing the security of the system.

The relationship between time-delay mismatch and BER is discussed, as shown in Fig. 9(a) and (b). The mismatch range is measured by adding a slight amount of detuning to T_3 and T_4 respectively at a legitimate receiver to observe the BER performance of the decrypted signal. Within the tolerant range of delay mismatch decided by the BER under the HD-FEC, for the legitimate receiver that has a slight parameter detuning, the whole system can work properly. But once beyond the limits of device parameters, as for the illegal eavesdropper, the BER of the illegally received becomes unacceptable. We can also observe from Fig. 9 that the tolerance range of time-delay mismatch is significantly reduced for larger modulation depths. When both β_1 and β_2 are equal to 1.5, the delay mismatch range of T_1 is about ± 10 ps. Further, when both β_1 and β_2 are increased to 2.4, the mismatch range of T_1 at this time is reduced to ± 5 ps. That significantly increases the requirement for equipment accuracy. More careful observation reveals the mismatch ranges of T_1 and T_2 are not obviously different, which is caused by the fact that both feedback branches are configured in the same structure, but this does not affect our exploration of the overall system regulation.

Besides the time-delay mismatch, the tolerance of dispersion was also an essential aspect we investigated. As the dispersion mismatch between D_2 and D_3 increases, the residual dispersion values can contribute to different conversion extent of PM-to-IM between the transmitting and receiving sides, leading to error codes. Consequences of D_2 and D_3 dispersion values detuning on BER are shown in Fig. 10. The maximum dispersion mismatch is approximately ± 40 ps/nm when both β_1 and β_2 are equal to 1.5. Modulation depth increases, which will make BER more susceptible to residual dispersion, decreasing the system's tolerance to dispersion by nearly ± 20 ps/nm. As the mismatch tolerance decreases, the hardware parameters of the transmitter and receiver must be more precisely matched, indicating the increase in modulation depth will raise the hardware parameter requirements at the legitimate receiver side. This fully validates the discussion in Part B that increasing the modulation depth will enhance the concealment effectiveness of the TDS, but the concomitant negative result is much stringent requirement on the components. Therefore, to maintain the best performance of the system, we must make a trade-off between TDS concealment and communication capability. Finally, after obtaining the detuning tolerance of each individual hardware parameter, the contribution of each parameter to the hardware key space can be calculated. In the current system parameter setting, the key space of the whole system is estimated to be $\sim 2^{25}$ in the case of $\beta_1 = \beta_2 = 1.5$, which can be further greatly improved by increasing the tuning range of each parameter. Compared to the traditional single-loop structure, the key space of the system is significantly enhanced, which provides an effective solution for secure communication.

IV. Conclusion

In summary, we proposed and numerically demonstrated a novel phase encryption scheme base on a dual-loop electro-optic

self-feedback structure, to achieve TDS concealment in the physical layer and investigated the performance of hardware parameters in detail. This remarkably enhances the security of electro-optic self-feedback-based communication systems and considerably reduces the threat from illegal eavesdroppers. We revealed how the modulation depth and dispersion values impact the TDS, which has positive implications for subsequent research on the selection of parameter values. In addition, the impact of hardware parameter mismatch on the BER of the system is investigated, and the results show the scheme has the ability to cope with the slight difference in the hardware parameters between commercial devices. The results highlight that the scheme can effectively accommodate slight hardware parameter variations between parts of commercial equipment. Further, the applicability of the scheme is also explored for phase modulation format, showing that it performs well even when transmitting phase information. Considering the advantages in the enhancement of security, along with the concise and practical implementing potential, it may induce a broader application of this dual-loop structure approach in the future.

REFERENCES

[1] N. Skorin-Kapov, M. Furdek, S. Zsigmond, and L. Wosinska, "Physical-layer security in evolving optical networks," *IEEE Commun. Mag.*, vol. 54, no. 8, pp. 110–117, Aug. 2016.

[2] N. Jiang, A. Zhao, Y. Wang, S. Liu, and K. Qiu, "Security-enhanced chaotic communications with optical temporal encryption based on phase modulation and phase-to-intensity conversion," *OSA Continuum*, vol. 2, no. 12, pp. 3423–3438, Dec. 2019.

[3] B. Wu, M. Chang, B. Shastri, P. Ma, and P. Prucnal, "Dispersion deployment and compensation for optical steganography based on noise," *IEEE Photon. Technol. Lett.*, vol. 28, no. 4, pp. 421–424, Feb. 2016.

[4] A. Argyris, E. Grivas, M. Hamacher, A. Bogris, and D. Syvridis, "Chaos-on-a-chip secures data transmission in optical fiber links," *Opt. Exp.*, vol. 18, no. 5, pp. 5188–5198, Mar. 2010.

[5] J. Bai, H. Wang, and Y. Ji, "Time-delay signature concealing electro-optic chaotic system with multiply feedback nonlinear loops," *Opt. Exp.*, vol. 29, no. 2, pp. 706–718, Jan. 2021.

[6] L. Pecora and T. Carroll, "Synchronization in chaotic systems," *Phys. Rev. Lett.*, vol. 6, no. 8, pp. 142–145, Jun. 1996.

[7] A. Argyris et al., "Chaos-based communications at high bit rates using commercial fiber-optic links," *Nature*, vol. 438, no. 7066, pp. 343–346, Nov. 2005.

[8] R. Lavrov, M. Jacquot, and L. Larger, "Nonlocal nonlinear electro-optic phase dynamics demonstrating 10 Gb/s chaos communications," *IEEE J. Quantum Electron.*, vol. 46, no. 10, pp. 1430–1435, Oct. 2010.

[9] T. Lu, H. Wang, and Y. Ji, "Wideband complex-enhanced bidirectional phase chaotic secure communication with time-delay signature concealment," *Chaos*, vol. 30, no. 9, Sep. 2020, Art. no. 093138.

[10] J. Ke et al., "32 Gb/s chaotic optical communications by deep-learning-based chaos synchronization," *Opt. Lett.*, vol. 44, no. 23, pp. 5776–5779, Dec. 2019.

[11] Z. Gao et al., "32 Gb/s physical-layer secure optical communication over 200 km based on temporal dispersion and self-feedback phase encryption," *Opt. Lett.*, vol. 47, no. 4, pp. 913–916, Feb. 2022.

[12] V. Annovazzi-Lodi and G. Aromataris, "Privacy in two-laser and three-laser chaos communications," *IEEE J. Quantum Electron.*, vol. 51, no. 7, Jul. 2015, Art. no. 7000405.

[13] D. Wang et al., "Time delay signature elimination of chaos in a semiconductor laser by dispersive feedback from a chirped FBG," *Opt. Exp.*, vol. 25, no. 10, pp. 10911–10924, May 2017.

[14] A. Wang, Y. Wang, Y. Yang, M. Zhang, H. Xu, and B. J. Wang, "Generation of flat-spectrum wideband chaos by fiber ring resonator," *Appl. Phys. Lett.*, vol. 102, no. 3, Jan. 2013, Art. no. 031112.

[15] S. Y. Xiang et al., "Wideband unpredictability-enhanced chaotic semiconductor lasers with dual-chaotic optical injections," *IEEE J. Quantum Electron.*, vol. 48, no. 8, pp. 1069–1076, Aug. 2012.

[16] H. Wang, T. Lu, and Y. Ji, "Key space enhancement of a chaos secure communication based on VCSELs with a common phase-modulated electro-optic feedback," *Opt. Exp.*, vol. 28, no. 16, pp. 23961–23977, Aug. 2020.

[17] N. Jiang, A. Zhao, C. Xue, J. Tang, and K. Qiu, "Physical secure optical communication based on private chaotic spectral phase encryption/decryption," *Opt. Lett.*, vol. 44, no. 7, pp. 1536–1539, Apr. 2019.

[18] G. Zou, H. Wang, and Y. Ji, "Electro-optic chaos system with time delay signature concealment based on XOR operation and multi-bit PRBS," *Opt. Exp.*, vol. 29, no. 5, pp. 7327–7341, Mar. 2021.

[19] R. M. Nguimdo, P. Colet, L. Larger, and L. Pesquera, "Digital key for chaos communication performing time delay concealment," *Phys. Rev. Lett.*, vol. 107, no. 3, Jul. 2011, Art. no. 034103.

[20] 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, Oct. 2015.

[21] X. Zhu et al., "An optically coupled electro-optic chaos system with suppressed time-delay signature," *IEEE Photon. J.*, vol. 9, no. 3, Jun. 2017, Art. no. 6601009.

[22] 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, no. 11, pp. 1306–1313, Nov. 2019.

[23] C. Wang, Y. Ji, H. Wang, and L. Bai, "Security-enhanced electro-optic feedback phase chaotic system based on nonlinear coupling of two delayed interfering branches," *IEEE Photon. J.*, vol. 10, no. 4, Aug. 2018, Art. no. 7203415.

[24] H. Huang, Z. Li, X. Gao, and M. Cheng, "An enhanced electro-optic chaos secure communication system immune to time delay signature extraction," *IEEE Photon. J.*, vol. 14, no. 1, Feb. 2022, Art. no. 7209407.

[25] Y. Lu, H. Wang, and Y. Ji, "A time-delay signature elimination and broadband electro-optic chaotic system with enhanced nonlinearity by deep learning," *Opt. Exp.*, vol. 30, no. 11, pp. 17698–17712, May 2022.

[26] R. Lavrov et al., "Electro-optic delay oscillator with nonlocal nonlinearity: Optical phase dynamics, chaos, and synchronization," *Phys. Rev. E*, vol. 80, no. 2, Aug. 2009, Art. no. 026207.

[27] Y. Ma et al., "Time-delay signature concealment of chaos and ultrafast decision making in mutually coupled semiconductor lasers with a phase-modulated Sagnac loop," *Opt. Exp.*, vol. 28, no. 2, pp. 1665–1678, Jan. 2020.