Optics Letters

Simplified coherent chaotic optical secure communication scheme based on the Kramers–Kronig receiver

Shuangquan Gu,[1,2] Pei Zhou,[1,2] Kuenyao Lau,[1,2] and Nianqiang Li[1,2,*]

[1]School of Optoelectronic Science and Engineering & Collaborative Innovation Center of Suzhou Nano Science and Technology, Soochow University, Suzhou 215006, China
[2]Key Lab of Advanced Optical Manufacturing Technologies of Jiangsu Province & Key Lab of Modern Optical Technologies of Education Ministry of China, Soochow University, Suzhou 215006, China
*wan_103301@163.com

Received 24 June 2024; revised 30 July 2024; accepted 31 July 2024; posted 2 August 2024; published 16 August 2024

Enhancing physical layer encryption in fiber-optic networks remains a challenging yet vital task. In this Letter, we propose a simplified coherent chaotic secure optical communication scheme based on the Kramers–Kronig (KK) receiver. This scheme incorporates a semiconductor laser with a phase-conjugated optical feedback serving as a common chaotic source, and its chaotic output is directly injected into the two slave lasers arranged separately at the transmitter and receiver end to achieve high-quality synchronization of chaotic signals, with a corresponding chaotic bandwidth of 30.6 GHz. By virtue of the common-signal-induced broad chaotic synchronization, a proof-of-principle demonstration is successfully conducted. It involves the secure transmission of a 20 Gbaud 16-level quadrature amplitude modulation (16QAM) signal over a 50 km standard single-mode fiber (SSMF) link. At the receiver end, we deploy a KK receiver to reconstruct the field of the optical signal and hence enable signal compensation and recovery with offline digital signal processing (DSP). This method simplifies device requirements in the current chaotic coherent optical secure communication, offering a cost-effective mode and promising path for advancing physical layer encryption in inter-data center communications.

https://doi.org/10.1364/OL.533696

The recent decade witnessed explosive growth in mobile Internet, big data, cloud computing, and artificial intelligence. This surge has driven the demand for data content and computing power, particularly in video services, increasingly toward data centers for processing. Ensuring the secure transmission of this data has become a crucial research focus. Various approaches have been explored to overcome this challenge, including quantum communications [1], optical code division multiple access [2], and chaotic communication [3–7]. Among them, chaotic secure communication, leveraging the inherent randomness and initial value sensitivity of chaotic signals, has emerged as a promising solution for physical layer encryption. In recent years, the field has been particularly focused on two primary objectives, i.e., high-speed transmission and long-distance secure communication. However, these goals may be hindered by challenges in generating broadband chaotic sources and maintaining long-range chaotic synchronization.

Consequently, to address these hurdles, Wang *et al.* and Yi *et al.* proposed incorporating the coherent detection technique into chaotic secure communication, marking a significant step forward in addressing these challenges. They validated the feasibility of this technique and demonstrated long-distance secure transmission through numerical simulations [8,9]. In the following year, Fu *et al.* demonstrated chaotic coherent secure optical communication over a 1600 km standard single-mode fiber (SSMF) with 5 Gbaud 16QAM signals through numerical simulations [10]. Yang *et al.* combined deep learning with coherent detection and experimentally achieved chaotic secure transmission of 30 Gb/s quadrature phase-shift keying (QPSK) signals over a 340 km SSMF [11]. In 2022, Wu *et al.* conducted an experimental implementation of 60 Gb/s encrypted QPSK signal transmission across a 100 km SSMF link with hybrid chaotic encryption harnessing one dual-polarization in-phase/quadrature modulator (I/Q Mod) [12]. In pursuing extended transmission distances and increased capacity, a plethora of pioneering strategies have been meticulously explored and investigated [13–17]. While these endeavors have undeniably propelled both distance and capacity forward, there remains an urgent demand to enhance system security, streamline implementation, and reduce costs, particularly in data center optical transmission systems. These systems necessitate solutions that are both power-efficient and cost-effective. Therefore, the pursuit of new and viable solutions to achieving large-capacity, lower-cost, and high-security transmission is paramount.

Motivated by the aforementioned issues, this Letter proposes a chaotic secure communication scheme that combines broad chaotic synchronization induced by the common chaotic signal originating from the semiconductor laser with a phase-conjugated optical feedback and the carrier-assisted direct detection using the Kramers–Kronig (KK) receiver [18]. A

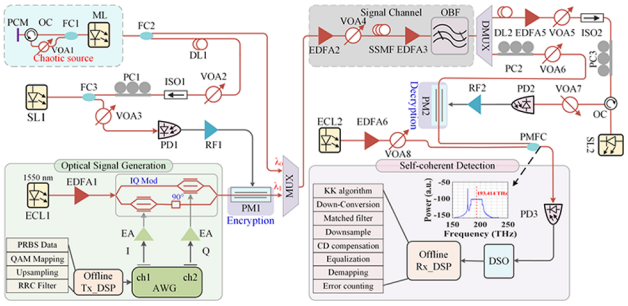

Fig. 1. Schematic diagram of the simulation device for self-coherent detection chaotic secure communication. PCM, phase-conjugated mirror; OC, optical circulator; FC, fiber coupler; VOA, variable optical attenuator; ISO, optical isolator; PC, polarization controller; SL, slave laser; ECL, external cavity laser; EA, electrical amplifier; RF, radio frequency amplifier; PM, phase modulator; AWG, arbitrary waveform generator; MUX, multiplexer; EDFA, erbium-doped fiber amplifier; IQ Mod, in-phase/quadrature modulator; SSMF, standard single-mode fiber; OBF, optical bandpass filter; DMUX, demultiplexer; DL, variable optical delay line; PD, photodetector; PMFC: polarization-maintaining fiber coupler; DSO, digital storage oscilloscope.

proof-of-principle demonstration by the secure transmission of a 20 Gbaud 16QAM data stream over a 50 km SSMF link is conducted numerically. The architecture of the proposed system consists of four main components, including a transmitter with chaotic phase encryption, an optical fiber link, a receiver with chaotic decryption, and self-coherent detection based on the KK receiver, as shown in Fig. 1.

At the transmitter end, the semiconductor master laser (ML) with a phase-conjugated optical feedback acts as the common chaotic source. The chaotic laser is then split into two parts through the fiber coupler (FC1), with one part injected into the slave laser (SL1) to generate the broad chaotic laser. This signal is then processed by a variable optical attenuator (VOA3) and a photodetector (PD1), transforming the optical signal into an electrical one. A radio frequency amplifier (RF1) controls the power of the electrical chaotic signal to drive the phase modulator (PM1), achieving the 16QAM optical signal phase encryption. The 16QAM optical signal generation process is as follows: a random function in MATLAB generates a bits sequence, which is then mapped to 16QAM symbols of length 2^{16}-length with a symbol rate of 20 Gbaud and up-sampled by a factor of 4 [19]. The resulting signal then undergoes transmission through a root-raised-cosine (RRC) pulse-shaping filter with a roll-off factor of 0.01. The real and imaginary components of the signal are loaded into the arbitrary waveform generator (AWG) and subsequently fed into an electrical amplifier to drive the IQ modulator. This modulates the continuous-wave light emitted from the external cavity semiconductor laser (ECL1) with a 100 kHz linewidth at 1550 nm. The 16QAM optical signal ($E_{\mathrm{sig}}(t)$) generated by the IQ modulator is expressed as follows:

$$E_{sig}(t) = A_{data}(t)\exp[j\varphi_{data}(t)], \tag{1}$$

where $A_{data}(t)$ and $\varphi_{data}(t)$ are the amplitude and phase of the data signal, respectively.

After the output light passes through the phase modulator (PM1), driven by the electrical chaotic signal, which originates from the optoelectronic conversion of the broadband chaotic laser by the photodetector (PD), the phase-encrypted signal ($E_{\mathrm{en}}(t)$) is denoted as follows:

$$\begin{cases} E_{en}(t) = E_{sig}(t)\exp(i\phi(t)) \\ \phi(t) = B \cdot LPF\{\dot{\mathbf{N}}[|E_{S1}(t)|^2]\}\pi \end{cases}. \tag{2}$$

Here, B is defined as the phase encryption depth, and LPF represents the first-order low-passband filtering with a cutoff frequency of 15 GHz due to the bandwidth limitation of the PD and RF1 [20]. $\dot{\mathbf{N}}[\cdot]$ represents the normalization, and more detailed information is described in [21]. Then, another chaotic laser from the FC2 is multiplexed with the encrypted signal by the wavelength division multiplexer (MUX) and sent into the SSMF link.

In the transmission link, the evolution of the light waves in the SSMF is molded by the nonlinear Schrödinger equation and calculated using the split-step Fourier method [22]. The SSMF parameters include the chromatic dispersion coefficient $\beta_2 = -20.0\ \mathrm{ps^2/km}$, the nonlinear parameter $\gamma = 1.3\ \mathrm{W^{-1}km^{-1}}$, and the loss coefficient $\alpha = 0.2\ \mathrm{dB/km}$ [9]. An erbium-doped fiber amplifier (EDFA2) and VOA4 are adopted to set the launch power before the SSMF to be 0 dBm, which can ensure a high signal-to-noise while achieving a low nonlinear effect. Then the optical power of the signal after the SSMF transmission is boosted by the EDFA3. A tunable optical bandpass filter (OBF) is used to remove the out-of-band amplified spontaneous emission noise.

At the receiver side, the phase-encrypted signal and the chaotic laser are demultiplexed by the demultiplexer (DMUX). The phase-encrypted signal is injected into slave laser 2 (SL2) to achieve broad chaotic synchronization and phase decryption. EDFA5 and VOA5 are combined to adjust the optical injection strength of the SL2. Subsequently, a continuous-wave optical carrier is emitted from ECL2 with the same parameters as the one at the transmitter side, with a center wavelength offset by 16 GHz. This carrier is combined with the decrypted signal by a polarization-maintaining fiber coupler (PMFC). The corresponding optical spectrum is shown in the inset of Fig. 1. The coupled signal is then detected by the PD3 and collected by a digital storage oscilloscope (DSO). Finally, the baseband signal is processed by the offline DSP, including the KK algorithm for reconstructing the optical field of the modulated signal, down-conversion, matched RRC filtering, down-sampling, chromatic dispersion (CD) compensation in the frequency domain, the constant modulus algorithm, and decision-directed least mean square. The original data stream is then recovered after QAM de-mapping and used for bit error rate (BER) evaluation.

In the simulation, the following modified Lang–Kobayashi equations are used to model the dynamics of the three lasers [23]:

$$\begin{aligned} \frac{dE_{M,S1,S2}(t)}{dt} = {} & \frac{1+i\alpha}{2}\left[G_{M,S1,S2}(t) - \frac{1}{\tau_p}\right]E_{M,S1,S2}(t) \\ & + k_f E_M^*(t-\tau_f)\exp(i\phi_{PCM}) \\ & + k_{inj1,2}E_M(t-\tau_{1,2})\exp[-i(2\pi f_M\tau_{1,2} - 2\pi\Delta f_{1,2}t)] \\ & + \sqrt{2\beta N_{M,S1,S2}(t)}\chi_{M,S1,S2}, \end{aligned} \tag{3}$$

$$\frac{dN_{M,S1,S2}(t)}{dt} = \frac{I_{M,S1,S2}}{q} - \frac{N_{M,S1,S2}(t)}{\tau_e} - G_{M,S1,S2}(t)|E_{M,S1,S2}(t)|^2, \tag{4}$$

$$G_{M,S1,S2}(t) = \frac{g[N_{M,S1,S2}(t) - N_0]}{1 + \varepsilon|E_{M,S1,S2}(t)|^2}. \tag{5}$$

Table 1. Parameters Used in the Simulations [23,24]

Parameter	Description	Value
α	Linewidth enhancement factor	5
τ_p	Photon lifetime	2 ps
τ_e	Carrier lifetime	2 ns
g	Differential gain coefficient	1.5×10^{-8} ps^{-1}
f_M	Center frequency of the ML	193.55 THz
N_0	Carrier transparency	1.5×10^8
β	Spontaneous emission factor	1.5×10^{-6} ns^{-1}
ε	Gain compression coefficient	5×10^{-7}
q	Electron charge	1.602×10^{-19} C
$k_{inj1,2}$	Injection strength of SL1,2	10 ns^{-1}
$\Delta_{f1.2}$	Frequency detuning between ML and SL1,2	30 GHz
k_f	Feedback strength	16 ns^{-1}
τ_f	Feedback time delay	3 ns
$\tau_{1,2}$	Injection delay time of SL1,2	3 ns
ϕ_{PCM}	Phase change of PCM	0 rad
I_{th}	Threshold current	14.7 mA
$I_{M,S1,S2}$	Injected current of ML, SL1, and SL2	$2.08I_{th}$

where the subscripts M, $S1$, and $S2$ represent the ML, SL1, and SL2, respectively. $E(t)$ is the complex electronic field amplitude, and $N(t)$ is the carrier number. E^* represents the complex conjugated electric field amplitude. $\chi_{M,S1,S2}$ is a Gaussian white noise with zero mean and unity variance, which is introduced to model the spontaneous emission noise. Table 1 offers a detailed description of the remaining parameters and their values in the simulations. The fine match of the injection delay time of SL1,2 is adjusted by the variable optical delay line (DL), as depicted in Fig. 1. In our simulation, Eqs. (3)–(5) are solved by using the fourth-order Runge–Kutta algorithm with a fixed time step of 1 ps.

It is notable that due to the conventional common injection-induced synchronization mechanism suffering from relatively high residual driving-response cross correlation [25], it may introduce a serious security risk of malicious attack by intercepting the common driving signal. To guarantee that the correlation between the ML and the SL response remains at a relatively low level, thus ensuring the security of the confidential information transmission, we refer to Fig. 4(a) in Ref. [23] and artificially set the frequency detuning between ML and both SLs to 30 GHz while maintaining their consistency [26], as shown in Table 1.

The correlation performance and the spectral characteristics of the chaotic signal at the transceiver side are analyzed. Figures 2(a1)–2(a3) display the intensity waveform of the ML, SL1, and SL2, respectively. The temporal waveform of the ML is completely different from the ones of the SL1 and SL2, whereas the time waveforms of the SL1 and SL2 exhibit almost the same fluctuation. Moreover, the correlation plots in Figs. 2(b1) and 2(b2) clearly show the low correlation between the ML and the SL, while the chaotic signals from both SLs at the transceiver side are well-synchronized, where the correlation is quantitatively characterized by the cross correlation coefficient (CC; see Eq. (7) in Ref. [27] for definition). A large CC value of 0.98 is realized between the two SLs, thanks to the common-chaotic-signal-induced synchronization mechanism, while the CC value between the ML and the SLs is only 0.1, again confirming the above elaboration. Meanwhile, Figs. 2(c1) and 2(c2) correspond

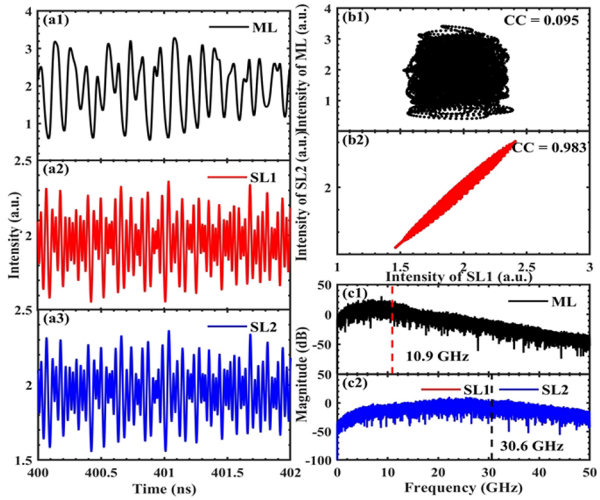

Fig. 2. Common-chaotic-signal-induced synchronization in semiconductor lasers. (a1)–(a3) Temporal waveforms, (b1)–(b2) correlation plots, (c1)–(c2) power spectra.

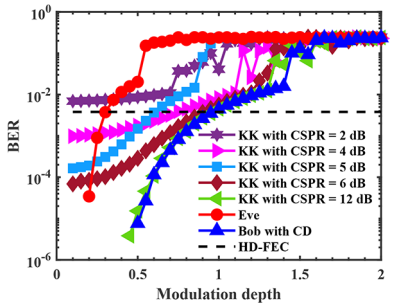

Fig. 3. BER versus modulation depth with different CSPR.

to the power spectra in Figs. 2(a1)–2(a3). The bandwidth of the ML is 10.9 GHz according to the 80% energy bandwidth definition [28]. The SL1 and SL2 show two almost identical power spectra with a higher bandwidth of 30.6 GHz due to the bandwidth enhancement effects of the optical injection [29].

In KK receivers, the carrier signal power ratio (CSPR) plays an essential role since this is only possible if the CSPR is high enough to maintain the minimum phase condition, which ensures a unique relationship between phase and amplitude. Here, the CSPR is defined as the power ratio of the CW from the ECL2 to the decrypted signal [30]. Moreover, the modulation depth of the PM1 and PM2 determines the security of information transmission in the proposed system. Therefore. we investigate the effect of the CSPR and modulation depth on the BER for legitimate users based on KK receivers (Bob with KK), as depicted in Fig. 3. Further, the effects of the modulation depth on the BER for illegal eavesdroppers (Eve) and legitimate receivers using conventional coherent detection (Bob with CD) are presented to facilitate comparison. The hard forward error correction (HD-FEC) limit (3.8×10^{-3}) is plotted in a black dotted line. It can be seen that chaotic phase encryption works only when the modulation depth is greater than 0.3, whereas, for a legitimate receiver, the encrypted information to be effectively recovered (Bob with CD) requires the modulation depth to be less than 0.95. Hence, we can extrapolate that varying the modulation depth from 0.3 to 0.95 ensures secure transmission

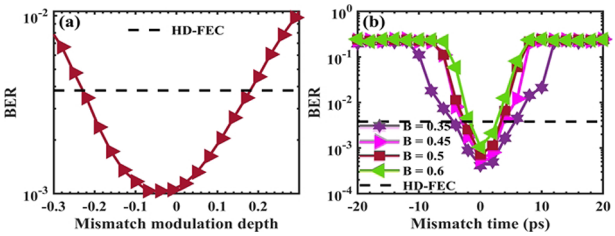

Fig. 4. BER performances for the mismatch of (a) phase modulation depths and (b) injection delay time.

and efficient recovery of information. Furthermore, the signal optical field can be effectively reconstructed only when the CSPR is greater than 2 dB. As the CSPR gradually increases, the BER is lowered for the same modulation depth. In the case of CSPR = 12 dB, a legitimate user with a KK receiver is capable of recovering the decrypted signal which resembles the one with a conventional coherent receiver (Bob with CD). However, the former is more simplified in terms of the device configuration, thus potentially reducing the cost. For trading off the power consumption and performance of the system, the optimized CSPR is chosen as 5 dB.

Finally, the effect of the parameter mismatch on the performance in this scheme is evaluated. Figure 4 shows the influence of the mismatch of the modulation depth as well as the injection delay time for different modulation depths between the transceivers on the BER. In this scenario, the parameters at the transmitter side are fixed where the modulation depth B = 0.6, and the mismatch is defined as the difference between the adjustable receive-side parameter and the transmit-side parameter. In Fig. 4(a), the modulation depth mismatch is in the range of −0.22–0.17 which guarantees secure transmission of information. On the other hand, the larger delay mismatch leads to the degradation of the decryption performance. Noticeably, when the delay time mismatch is less than 6 ps, a BER below the HD-FEC threshold can be obtained. Lower phase modulation depth leads to higher delay time errors. When the modulation depth is varied, the delay time error tolerance is observed to be 4–10 ps, as illustrated in Fig. 4(b). These results show that the performance of the proposed scheme is very sensitive to the mismatch in the delay time. Therefore, an adjustable delay line with a high resolution of 1 ps is required to minimize the delay time mismatch and guarantee the decryption performance.

In this Letter, we have numerically demonstrated a simplified coherent chaotic optical secure communication scheme, where a semiconductor laser with a phase-conjugated feedback, as a common chaotic source, is leveraged to trigger the generation of chaotic signals with large bandwidth and high-quality synchronization performance from a laser arranged at the transceiver end. Thanks to this synchronization mechanism, the phase en-/decryption of a 20 Gbaud 16QAM is achieved over a 50 km SSMF link by using a PD and a simpler digital post-processing (KK algorithm), which reduces the number of complex optical components required in conventional coherent receiver systems. Specifically, the KK receiver requires only one PD, whereas a 90° optical hybrid and four PDs are desired for a single-polarization coherent receiver system. Therefore, this work proposes a feasible and cost-effective method to facilitate secure communication at the physical layer between data centers.

Funding. National Natural Science Foundation of China (62001317, 62171305); Innovative and Entrepreneurial Talent Program of Jiangsu Province (JSSCRC2021527); Postgraduate Research & Practice Innovation Program of Jiangsu Province (KYCX24_3297).

Disclosures. The authors declare no conflicts of interest.

Data availability. Data underlying the results presented in this Letter are not publicly available at this time but may be obtained from the authors upon reasonable request.

REFERENCES

1. T. A. Eriksson, T. Hirano, B. J. Puttnam, *et al.*, Commun. Phys. **2**, 9 (2019).
2. Z. Jiang, D. E. Leaird, and A. M. Weiner, J. Lightwave Technol. **24**, 4228 (2006).
3. Z. S. Gao, Y. Luo, L. H. Zhang, *et al.*, Opt. Express **31**, 1666 (2023).
4. S. Xiang, M. Yang, and J. Wang, Opt. Lett. **47**, 2818 (2022).
5. H. Wang, T. Lu, and Y. Ji, Opt. Express **28**, 23961 (2020).
6. P. Didier, S. Zaminga, O. Spitz, *et al.*, Optica **11**, 626 (2024).
7. A. Argyris, D. Syvridis, L. Larger, *et al.*, Nature **438**, 343 (2005).
8. L. S. Wang, X. X. Mao, A. B. Wang, *et al.*, Opt. Lett. **45**, 4762 (2020).
9. Z. Yang, L. L. Yi, J. X. Ke, *et al.*, J. Lightwave Technol. **38**, 4648 (2020).
10. Y. D. Fu, M. F. Cheng, W. D. Shao, *et al.*, Opt. Lett. **46**, 1506 (2021).
11. Z. Yang, J. X. Ke, Q. B. Zhuge, *et al.*, Opt. Lett. **47**, 2650 (2022).
12. Y. Q. Wu, H. W. Luo, L. Deng, *et al.*, Opt. Lett. **47**, 5285 (2022).
13. L. Jiang, L. Yan, A. Yi, *et al.*, Opt. Express **28**, 302 (2020).
14. Y. Q. Wu, H. W. Luo, M. F. Cheng, *et al.*, Opt. Lett. **47**, 726 (2022).
15. Y. Q. Wu, Z. H. Zhang, H. W. Luo, *et al.*, Opt. Express **31**, 33200 (2023).
16. Y. Xie, Z. Yang, M. Shi, *et al.*, Adv. Photonics Nexus **3**, 016003 (2023).
17. X. Gao, W. Gu, Z. Deng, *et al.*, IEEE Photonics Technol. Lett. **36**, 481 (2024).
18. A. Mecozzi, C. Antonelli, and M. Shtaif, Optica **3**, 1220 (2016).
19. T. Bo and H. Kim, Opt. Express **26**, 13810 (2018).
20. T. Aida and P. Davis, IEEE J. Quantum Electron. **28**, 686 (1992).
21. N. Jiang, A. Zhao, S. Liu, *et al.*, Opt. Express **26**, 32404 (2018).
22. R. M. Nguimdo, R. Lavrov, P. Colet, *et al.*, J. Lightwave Technol. **28**, 2688 (2010).
23. N. Jiang, A. Zhao, S. Liu, *et al.*, Opt. Express **28**, 9477 (2020).
24. Y. Huang, P. Zhou, Y. Zeng, *et al.*, Phys. Rev. A **105**, 043521 (2022).
25. T. Yamamoto, I. Oowada, H. Yip, *et al.*, Opt. Express **15**, 3974 (2007).
26. N. Suzuki, T. Hida, M. Tomiyama, *et al.*, IEEE J. Sel. Top. Quantum Electron. **23**, 1 (2017).
27. Y. Zeng, Y. Huang, P. Zhou, *et al.*, Opt. Express **31**, 16178 (2023).
28. F. Y. Lin and J. M. Liu, Opt. Commun. **221**, 173 (2003).
29. A. B. Wang, Y. C. Wang, and J. F. Wang, Opt. Lett. **34**, 1144 (2009).
30. S. An, Q. Zhu, J. Li, *et al.*, J. Lightwave Technol. **38**, 485 (2020).