PHOTONICS Research

10 Gb/s classical secure key distribution based on temporal steganography and private chaotic phase scrambling

Zhensen Gao,[1,2,3] Zhitao Deng,[1] Lihong Zhang,[1] Xulin Gao,[1] Yuehua An,[4] Anbang Wang,[1,3] Songnian Fu,[1,2,3] Zhaohui Li,[2,5] Yuncai Wang,[1,2,3,*] and Yuwen Qin[1,3]

[1]School of Information Engineering, Guangdong University of Technology, Guangzhou 510006, China
[2]Pengcheng Laboratory, Shenzhen 518062, China
[3]Key Laboratory of Photonic Technology for Integrated Communication and Sensing, Ministry of Education, Guangzhou 510006, China
[4]School of Optoelectronic Engineering, Guangdong Polytechnic Normal University, Guangzhou 510665, China
[5]School of Electrical and Information Technology, Sun Yat-sen University, Guangzhou 510006, China
*Corresponding author: wangyc@gdut.edu.cn

Received 9 August 2023; revised 30 October 2023; accepted 13 November 2023; posted 14 November 2023 (Doc. ID 502992); published 1 February 2024

Secure distribution of high-speed digital encryption/decryption keys over a classical fiber channel is strongly pursued for realizing perfect secrecy communication systems. However, it is still challenging to achieve a secret key rate in the order of tens of gigabits per second to be comparable with the bit rate of commercial fiber-optic systems. In this paper, we propose and experimentally demonstrate a novel solution for high-speed secure key distribution based on temporal steganography and private chaotic phase scrambling in the classical physical layer. The encryption key is temporally concealed into the background noise in the time domain and randomly phase scrambled bit-by-bit by a private chaotic signal, which provides two layers of enhanced security to guarantee the privacy of key distribution while providing a high secret key rate. We experimentally achieved a record classical secret key rate of 10 Gb/s with a bit error rate lower than the hard-decision forward error correction (HD-FEC) over a 40 km standard single mode fiber. The proposed solution holds great promise for achieving high-speed key distribution in the classical fiber channel by combining steganographic transmission and chaotic scrambling.

https://doi.org/10.1364/PRJ.502992

1. INTRODUCTION

Nowadays, with the rapid development of various advanced modulation and multiplexing technologies, the capacity of fiber-optic networks has witnessed tremendous progress [1,2]. However, versatile increasing attacks seriously threaten fiber-optic network security, not only from the upper layer network attack but also from the lowest physical layer interception [3–6]. It is imperative to develop secure communication technologies to protect confidential data from eavesdropping.

Secure key distribution (SKD) is the main bottleneck for secure communication. To establish unconditional symmetric secure communication, a private key has to be shared securely between two authorized parties and combined with the one-time pad data encryption method [7]. For such an absolutely secure encryption method, it is expected that the secret key rate should be matched with the bit rate of the confidential data. Hence, achieving high-speed secure key distribution is an indispensable and quite challenging task for high-speed secure communication [8–10].

Traditionally, SKD is conducted by mathematical algorithms relying on computational security, but it is facing the risk of exhaustive attacks by the rapid growth of supercomputing [11,12]. As a physical layer SKD technology, quantum key distribution (QKD) allows two authorized parties to share a secret key via a quantum channel with unconditional security based on quantum mechanics, but it suffers from the limitation of key rate-distance product and incompatibility with commercial fiber-optic links [13,14]. It hence stimulates researchers to explore high-speed secure key distribution technologies based on classical optical fiber channels.

Several typical approaches have been previously reported for classical physical layer key distribution, including fiber-laser [15–19], fiber channel features [20–22], and optical chaos [23–42]. The fiber-laser-based approach enables secret key exchange by randomly selecting the laser cavity length or laser wavelength so that two distant users can share the secret key whenever the variables coincide with each other [15–19]. However, the key rate restricted by the variable switching speed

and long laser cavity can only reach ~100 b/s [16]. For the fiber channel feature approach, the secret key is extracted from highly correlated noise due to channel reciprocity based on optical phase [20], polarization mode dispersion [21], polarization fluctuation [22,23], etc. Because of the relatively slow channel feature fluctuation, the key rate is generally limited to the magnitude of Mb/s [22]. Although active perturbation methods were proposed to accelerate the fluctuation and increase the key rate [22,23], providing a high secret key rate of up to 10 Gb/s remains a challenge.

Alternatively, thanks to the rapid fluctuation and broadband nature of optical chaos [24–26], secret key distribution based on chaos synchronization was proposed as a very attractive way for classical key distribution, which provides a high key rate of up to Gb/s [27–42]. The most widely employed scheme is the common-signal-induced chaos synchronization, which generates a pair of consistent keys from remote synchronized optical chaos due to the common driving of a public random source [31–37]. It has been demonstrated that both the chaotic laser and optoelectronic oscillator could be used as the chaotic response source in the traditional common-driving response architecture [31–42]. Due to the limitation of laser relaxation oscillation frequency [24], the laser chaos-based response scheme only supports a key rate of a few Gb/s [31–33]. For using optoelectronic oscillators that could release the relaxation oscillation frequency limitation, a high key rate of 6 Gb/s is predicted but has not been experimentally demonstrated yet [38]. On the other hand, the security of the common driving-response architecture for correlated key generation strongly relies on the cross-correlation between the common driving signal and response chaotic signal, as well as the practical difficulty of manufacturing a hardware matched chaotic response source [31–42]. Unfortunately, security vulnerabilities have been revealed due to the relatively high driving-response correlation for most conventional schemes and rather limited hardware key space for chaotic response sources [31–37]. Furthermore, the common driving source should be placed in a third-party node in the transmission link, which induces the potential security risk of hijacking and adds complexity of network management.

Besides distilling secret keys from random chaotic signal based on chaos synchronization, optical chaos has also been proposed and demonstrated for chaotic phase scrambling to enable confidential signal transmission by encrypting a message as a noise-like signal [43–45]. Jiang *et al.* first introduced and numerically demonstrated chaotic spectral phase scrambling based on synchronized optical chaos for physical secure communication [43]. We have reported an experimental demonstration of the chaotic phase scrambling for encryption of a 28 Gb/s on-off-keying signal [44]. Zhao *et al.* have further demonstrated a secure wavelength-division multiplexing (WDM) system based on multi-channel spectral aliasing by chaotic phase scrambling induced spectral broadening [45]. Compared with intensity scrambling, chaotic phase scrambling is superior in terms of easier implementation without the subtraction operation for descrambling, enablement of reversible processing using off-the-shelf phase modulation components, transformability to intensity scrambling assisted by chromatic dispersion, and enhanced security by optical phase processing that is not easily discovered by an eavesdropper, but it would become ineffective for a stand-alone intensity modulated signal. Instead of scrambling a signal against malicious attacks, concealing a signal in either time or spectral domain by optical steganography is another extremely attractive way, which makes an eavesdropper unknow the existence of the confidential signal, not even to attack it. Steganographic transmission of a 500 Mb/s message with amplified spontaneous emission noise as a carrier has been successfully demonstrated [46].

In this paper, inspired by previous pioneering works, we propose and experimentally demonstrate a new way for high-speed secure key distribution based on temporal steganography and private chaotic phase scrambling. The secret key is temporally concealed into a private chaotic signal in the time domain and randomly phase scrambled bit-by-bit by the chaotic signal before distributing to the classical fiber channel. A semiconductor laser cascaded with an electro-optic phase feedback loop structure is employed as a chaotic source to generate the private chaotic scrambling signal. A single phase modulator is employed to simultaneously perform chaotic phase scrambling and secret key modulation. The phase scrambled secret key is temporally kept constant to enable steganographic transmission without the awareness of an eavesdropper. The security of the secret key is double guaranteed by the first level of unawareness by temporal steganography and the second level of private chaotic phase scrambling. Based on this solution, we successfully demonstrate a record high secret key rate of 10 Gb/s over a 40 km classical standard single mode fiber (SSMF) link with a bit-error-rate (BER) below the 7% HD-FEC limit of 3.8×10^{-3}.

2. PRINCIPLE AND EXPERIMENTAL SETUP

The schematic diagram of the proposed high-speed secure key distribution scheme over classical fiber channels is illustrated in Fig. 1. In this scheme, a chaos synchronization channel is employed to provide a pair of distributed private chaotic signals by injecting a common driving signal from a driving laser (DL) into a twin of private response chaotic modules (PRCMs) located at the legitimate users' sides (Alice and Bob). The PRCM guarantees that the generated private chaotic signal has extremely low correlation with the common driving signal exposed in the public channel and provides hardware security against a malicious eavesdropper's attack. At the secure key distribution (SKD) channel, a true random key generator (TRKG) first generates a secret digital key to be distributed, which is then mixed with the private chaotic signal coming from the

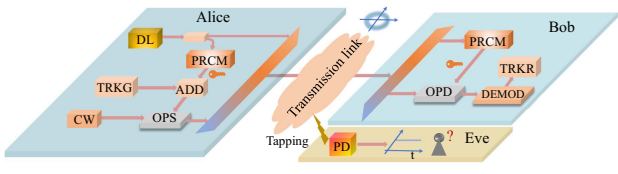

Fig. 1. Schematic diagram of the proposed classical secure key distribution scheme. DL, driving laser; PRCM, private response chaotic module; TRKG, true random key generator; CW, continuous-wave laser; OPS, optical phase scrambler; OPD, optical phase descrambler; TRKR, true random key receiver; PD, photo-detector.

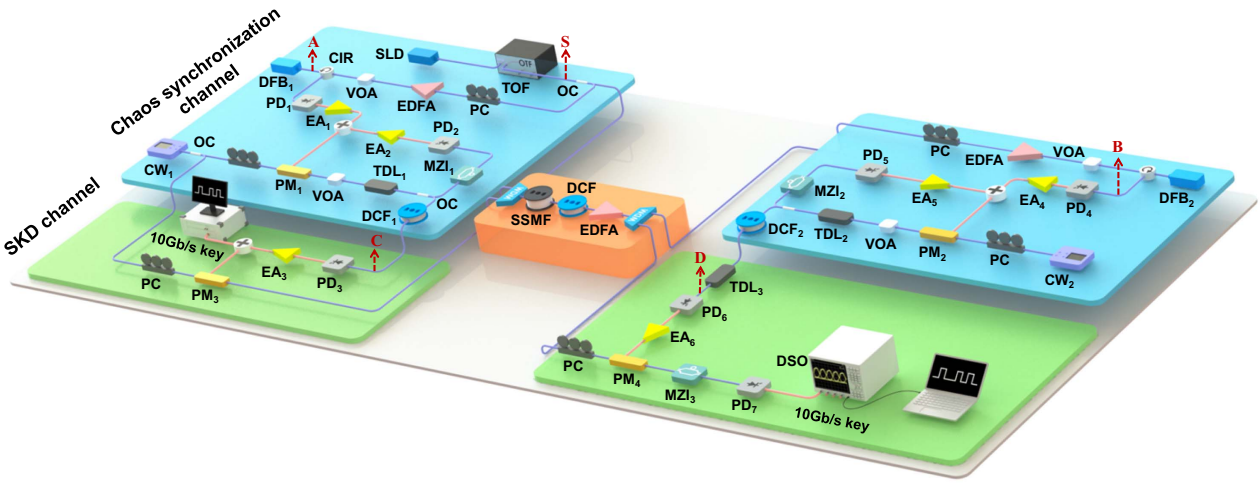

Fig. 2. Experimental setup of the proposed high-speed secure key distribution scheme. SLD, super-luminescent diode; TOF, tunable optical filter; DFB, distributed feedback laser; CW, continuous-wave laser; OC, optical coupler; VOA, variable optical attenuator; PC, polarization controller; CIR, circulator; EDFA, erbium-doped-fiber-amplifier; PD, photo-detector; EA, electrical amplifier; MZI, Mach–Zehnder interferometer; DCF, dispersion compensation fiber; TDL, tunable delay line; PM, phase modulator; DSO, digital sampling oscilloscope.

PRCM at Alice's side, so that the digital key is temporally concealed into the random fluctuated private chaotic signal for steganographic distribution. The mixed signal is further imposed onto an optical phase scrambler (OPS) seeded by a separate continuous-wave laser (CW) to simultaneously perform digital key modulation and chaotic phase scrambling of the secret key using a single optical module.

At Bob's side, the hardware matched PRCM similarly generates the synchronized private chaotic signal, which is imposed onto an optical phase descrambler (OPD) to descramble the random phase of the received distribution signal. The resulting phase descrambled signal is further demodulated and directed into a true random key receiver (TRKR), accomplishing the secret key distribution process, which provides dual-level of security provided by temporal steganography and private chaotic phase scrambling. Since the distributed signal at the SKD channel is randomly phase scrambled and temporally exhibits as a constant background noise, it is difficult for Eve to be aware of the existence of the secret digital key by just performing direct-detection attack using a simple photo-detector (PD) in the transmission link. Moreover, even if a sophisticated Eve notices the existence of the secret key and attempts to attack the system by tapping the common driving signal for phase descrambling or directly applying phase demodulation techniques, the distributed key is still kept secret as long as the PRCM hardware is not revealed to Eve in the scheme.

Figure 2 shows the experimental setup of the proposed secure key distribution scheme. The chaos synchronization channel and SKD channel are combined together via wavelength-division multiplexing for secure key distribution. As for the chaos synchronization channel, a super-luminescent diode (SLD) followed by a tunable optical filter (TOF) with a 3 dB bandwidth of ~0.5 nm and center wavelength of 1549.98 nm is utilized as a common driving source. A 3 dB optical coupler (OC) is then used to split the driving signal into two portions, which are independently injected into the private response chaotic modules located at Alice and Bob, respectively. Each PRCM consists of a distributed-feedback (DFB) laser and an electro-optic phase feedback loop to greatly suppress the driving-response cross-correlation and enhance the hardware key space, which further guarantees the privacy of the generated chaotic signal from both the transmission link and the local hardware chaotic source. The wavelengths of the two DFB lasers for Alice and Bob are finely adjusted to be assigned an identical wavelength of 1549.91 nm. The threshold currents for DFB_1 and DFB_2 are measured as 11.38 mA and 10.38 mA. The driving currents for DFB_1 and DFB_2 are both biased at 1.3 times the threshold currents. The temperatures for the two lasers are set as 21°C and 18.3°C, respectively. Two erbium-doped optical fiber amplifiers (EDFAs) are employed to control the injection strengths of the driving signal to achieve chaos synchronization based on common injection induced synchronization. The injection strengths for DFB_1 and DFB_2 are 0.39 and 0.41, respectively.

At each legitimate user's side, the synchronized chaotic signal output from the response DFB lasers ($DFB_{1,2}$) is directly injected into an electro-optic phase feedback loop, which comprises a phase modulator (PM), a variable optical attenuator (VOA), a tunable optical delay line (TDL), a Mach–Zehnder interferometer (MZI), a photo-detector (PD), and an electrical amplifier (EA). An external-cavity continuous wave laser (CW_1) with a center wavelength of 1550.92 nm and a narrow linewidth of ~100 kHz is shared as the seed light by the chaos synchronization channel and secure key distribution channel at Alice's side. The continuous wave generated by the CW_1 is first phase modulated by the synchronized chaotic signal output from DFB_1 and then intentionally time delayed by TDL_1 before splitting into two portions by a 50:50 optical coupler (OC), one of which is transformed into a feedback intensity scrambled chaotic signal by MZI_1 with a free spectral range (FSR) of 10 GHz and converted into an electrical signal by PD_1. The intensity scrambled chaotic signal is further com-

bined with the externally injected chaotic signal by a power combiner and is eventually fed back to drive the phase modulator so that the intensity combined signal is converted into a new phase scrambled signal, which forms a recirculating phase feedback loop. In contrast, the other portion is directed into a dispersive component to generate the private chaotic scrambling signal. A piece of dispersion compensation fiber (DCF_1) can be used as the dispersive component. Thanks to the random phase modulation to intensity perturbation conversion due to the chromatic dispersion introduced by the dispersive fiber [43], the private phase scrambled signal after PM_1 is transformed into another intensity scrambled chaotic signal for further photo-detection and phase scrambling of the secret digital key. In the setup, the bandwidth and half-wave voltage of the PM are 10 GHz and 3.3 V. The 3 dB bandwidth for the PDs is 10 GHz. The EAs are low noise electrical amplifiers (Connphy CLN-3545) with a 3 dB bandwidth of 30 GHz. The total time delay of the feedback loop is around 69.54 ns, which can be flexibly adjusted by the TDL_1. The dispersion of the DCF_1 is around −1000 ps/nm. The key hardware parameter values of the feedback loop and the physical parameters of the DFB response lasers contribute together to ensure the privacy of the output chaotic scrambling signal.

Afterward, the generated chaotic scrambling signal from the phase feedback loop is converted to an electrical signal by PD_3, amplified by AMP_3, and then combined with the electrical digital key sequence by a power combiner to conceal the secret key in the time domain. Variable electrical attenuators are employed to precisely control the concealment coefficient (α), which is defined as the power ratio between the digital secret key sequence and the chaotic scrambling signal. Practically, the secret key can be generated by a true random number generator. To emulate the digital secret key, a pseudo-random binary sequence (PRBS) of $2^{23}-1$ generated by an arbitrary waveform generator (Keysight AWG 8195A) is utilized in this scheme. The temporally concealed digital key sequence is then applied into another phase modulator (PM_3) to perform phase shift keying modulation so that the secret key is further concealed into the private chaotic signal in the phase domain. Since the phase modulated combined signal temporally exhibits as an intensity constant background noise, a malicious eavesdropper will be unaware of the existence of the secret key sequence that is concealed into the private chaotic signal to enable temporal steganographic transmission. More importantly, thanks to the unpredictable and non-reproducible features of optical chaos [24–26], the phase of the secret digital key sequence is randomly scrambled bit-by-bit by the private chaotic scrambling signal, which is equivalent to the digital "one-time-pad" cryptography counterpart but is implemented in the optical domain for realizing high-speed classical secure key distribution. Unlike the previous chaotic phase scrambling induced spectral aliasing mechanism that is effective for the multi-channel WDM environment [45], the current scheme can be flexibly adapted to either single- or multi-channel systems, and notably only a single phase modulator is employed to simultaneously perform digital secret key modulation and private chaotic phase scrambling. Based on this scheme, the security of the key distribution is double guaranteed by the first level of temporal unawareness and the second level of private chaotic phase scrambling. After that, the chaotic phase scrambled secret signal is distributed over a 40 km standard single mode fiber (SMF) followed by a span of 6.4 km DCF for dispersion compensation.

At the authorized user Bob's side, the common driving signal is first wavelength demultiplexed from the received signal and then injected into the chaotic response source comprising a DFB_2 and a hardware matched electro-optic phase feedback loop to generate a private synchronized chaotic optical signal, which is further converted into an electrical chaotic signal by PD_6. The output synchronized signal from the inverse output port of the PD_6 is then amplified to drive the PM_4 so that the received chaotic phase scrambled secret signal is phase descrambled by the remotely generated private chaotic descrambling signal, unveiling the secure phase modulated key sequence in the SKD channel. A tunable delay line (TDL_3) is used to temporally align the timing mismatch between the private chaotic descrambling signal and the secure key distribution signal. The phase modulated secret key is finally extracted by MZI_3 with an FSR of 10 GHz and thus successfully distributed to Bob. A malicious eavesdropper without any knowledge of the proper hardware parameters will be unable to counterfeit a matched chaotic response source and intercept the private chaotic descrambling signal, which provides hardware security to enable secure distribution of the secret key.

3. RESULTS AND DISCUSSION

A. Chaos Correlation Performance

To guarantee the privacy of the chaotic scrambling signal and ensure high-speed secure key distribution, it is essential to investigate the chaos correlation performance at different stages in the chaos synchronization channel. A high synchronization coefficient could lead to a reduced key distribution error, and a low driving-response cross-correlation coefficient would result in enhanced scrambling security. Figures 3(a)–3(h) illustrate the measured temporal waveforms and the corresponding cross-correlation plots measured at different positions in Fig. 2, respectively. When the common driving signal is directly injected into the response DFB lasers, it is clear that the temporal waveforms of the output chaotic signals from $DFB_{1,2}$ at positions A and B show strong dependence on the source driving signal at position S, as illustrated in Figs. 3(a) and 3(b). A high driving-response cross-correlation coefficient (C.C), which can be calculated by $C.C = \langle [S(t) - \langle S(t)\rangle] \cdot [A(t) - \langle A(t)\rangle]\rangle / \sqrt{\langle [S(t) - \langle S(t)\rangle]^2\rangle \cdot \langle [A(t) - \langle A(t)\rangle]^2\rangle}$, where $S(t)$ and $A(t)$ represent the temporal waveforms of the source driving and response signals, is measured to be as high as 0.41, indicating the serious security risk of eavesdropping by simply intercepting the driving signal for private chaotic phase scrambling. The correlation performance between the two synchronized output waveforms of $DFB_{1,2}$ at A and B is shown in Figs. 3(c) and 3(d), which exhibits high resemblance between each other and a high synchronization correlation coefficient of ~0.96. Benefiting from the nonlinear waveform transformation due to the phase to intensity conversion introduced by the electro-optic phase feedback loops, the eventual waveforms of the chaotic scrambling signals output from the response chaotic sources at C and D are entirely distinct from that of the

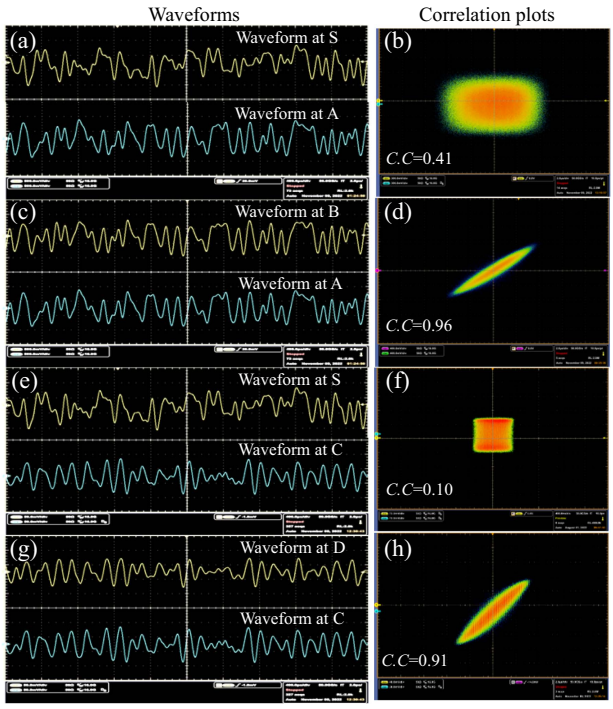

Fig. 3. Temporal waveforms (left column) and corresponding correlation plots (right column) of the output chaos measured at points (a), (b) *S* and *A*, (c), (d) *A* and *B*, (e), (f) *S* and *C*, and (g), (h) *C* and *D*, respectively.

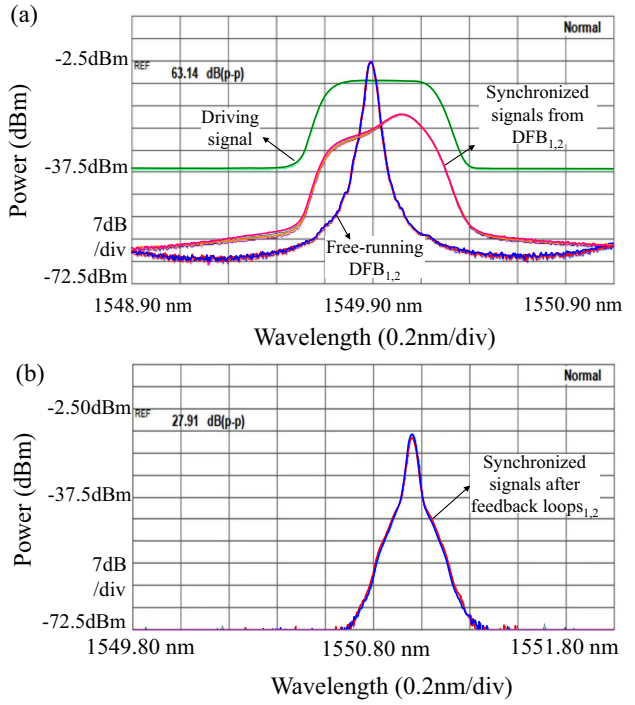

Fig. 4. (a) Optical spectra for the driving signal, free-running response signals, and synchronized signals from DFB lasers and (b) the synchronized chaotic scrambling signals after feedback loops.

common driving signal at *S*, as shown in Fig. 3(e). Compared with the case of direct injection into open-looped DFB response laser induced synchronization that has a relatively high residual correlation, as shown in Figs. 3(a) and 3(b), the residual cross-correlation by introducing the electro-optic phase feedback loops can be significantly reduced down to ∼0.1, which is plotted in Fig. 3(f), indicating that there is no private chaotic scrambling signal related information exposing in the public link so as to sufficiently guarantee the security of key distribution. It is also noted that the eventual output chaotic signals at points *C* and *D* are still highly correlated with each other, with a high correlation coefficient of ∼0.91, showing that high-quality chaos synchronization between the chaotic scrambling/descrambling signals is maintained, as illustrated in Figs. 3(g) and 3(h).

Figures 4(a) and 4(b) show the corresponding optical spectra measured at different points in the experimental setup. It is evident that the optical spectra of the chaotic signal output from the $DFB_{1,2}$ exhibits similar profiles due to the common noise-signal driving induced synchronization. Compared with free-running DFB lasers, the synchronized output signals are slightly broadened and red shifted due to the external injection [47]. Similarly, after the nonlinear transformation by the electro-optic phase feedback loops, the optical spectra for the eventual output chaotic signals still match well with each other, revealing that the private chaotic scrambling/descrambling signals are well synchronized.

Having observed the chaotic waveforms and optical spectra, attention is now focused on the relationship between the cross-correlation performances and the key hardware parameters in the setup. Figures 5(a) and 5(b) show the contour plots of the synchronization (points *C* and *D*) and driving-response cross-correlation coefficients (points *S* and *C*) versus the phase modulation depth of $PM_{1,2}$ and absolute dispersion value of the dispersive components. It can be seen from Fig. 5(a) that the phase modulation depth dominates the synchronization coefficient, which requires a minimum value of ∼0.88 to ensure a key distribution error rate lower than the 7% HD-FEC in this system. Increasing the phase modulation depth leads to the reduction of driving-response cross-correlation and thus enhancement of the security, but it would gradually degrade the synchronization coefficient accordingly, as shown in Figs. 5(a) and 5(b). In contrast, the dispersion has a trivial effect on the synchronization, but increasing it could dramatically reduce the residual driving-response cross-correlation to be lower than ∼0.1, which corresponds to an ultralow mutual information of ∼0.015 bit between the common driving and private chaotic scrambling signal to sufficiently guarantee the security.

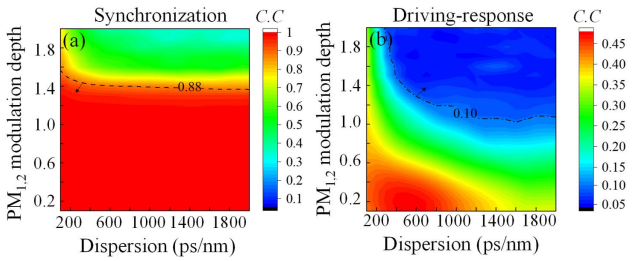

Fig. 5. (a) Synchronization coefficient and (b) residual driving-response cross-correlation versus PM modulation depth and dispersion.

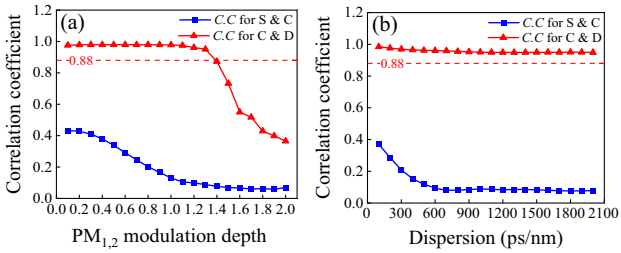

Fig. 6. (a) Correlation coefficients for different points versus the PM modulation depth and (b) DCF dispersion.

Figure 6(a) plots the cross-correlation coefficients versus the $PM_{1,2}$ modulation depth for a fixed dispersion value of 1000 ps/nm. It is clear that, with the increase of the modulation depth upon 1.1, the residual driving-response cross-correlation is gradually reduced down from 0.4 to 0.1, while the synchronization coefficient keeps still above 0.88. Further increment of the PM modulation depth would result in the reduction of the synchronization coefficient. When the PM modulation depth surpasses 1.4, the synchronization coefficient becomes lower than 0.88. Hence, the PM modulation depth is controlled to be around 1.1–1.4 to simultaneously guarantee the synchronization performance and security. Figure 6(b) depicts the correlation coefficients versus the dispersion for a fixed PM modulation depth of 1.2. When increasing the dispersion, the synchronization coefficient keeps stably above 0.88, but the residual driving-response correlation coefficient gradually decreases down to a plateau of ~0.05. A minimum dispersion value of ~600 ps/nm is required to reduce the residual driving-response correlation lower than ~0.1 in the system. Therefore, a DCF with an absolute dispersion value of ~1000 ps/nm is utilized in the system to satisfy the requirement.

B. Tolerance of Hardware Parameters Mismatch

In addition, since the key hardware parameters including the DFB laser inner parameters, DCF dispersion, feedback loop delay time, PM modulation depth, and MZI interference delay time are the most important factors that determine the chaos synchronization performance, it is quite essential to evaluate the tolerances of these hardware parameters mismatch. As a fundamental layer of hardware security, a pair of parameter-matched DFB lasers is desired for legitimate users to achieve high-quality chaos synchronization. The mismatch of DFB laser parameters would inevitably have impact on the synchronization coefficient and thus the key distribution performance. Figure 7 shows the effects of synchronization coefficient on the mismatch of DFB laser inner parameters, which mainly takes the linewidth enhancement factor α, active region length L_a, linear gain coefficient g_n, carrier density at transparency N_0, and carrier capture time τ_c into account [25]. It has been found that the tolerances of laser parameters mismatch for α, L_a, g_n, N_0, and τ_c are around −0.880%–0.827%, −0.141%–0.140%, −1.33%–1.16%, −0.404%–0.317%, and −0.458%–0.440%, respectively. The maximum tolerable mismatch is lower than ±2%, indicating that two DFB lasers should be produced by using the same fabrication wafer in order to achieve high-quality chaos synchronization between

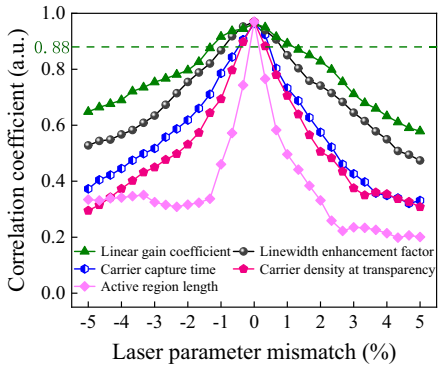

Fig. 7. Effects of DFB laser inner parameters mismatch on chaos synchronization.

legitimate users and also to prevent an eavesdropper from accessing a third laser with highly matched laser inner parameters.

Figures 8(a)–8(d) further show the correlation coefficients at points C and D versus the other key hardware parameter mismatch. It is apparent that any external hardware parameter detuning would cause the degradation of synchronization coefficient between the chaotic scrambling/descrambling signals. For a synchronization coefficient reduction to ~0.88, the mismatch tolerance for the dispersion is ~120 ps/nm, the feedback loop delay time is ~12 ps, the PM modulation depth is ~0.25, and the MZI interference delay time is ~300 fs, respectively. The relatively sensitive external hardware parameters could contribute to enhancing the security against an eavesdropper's attack, but meanwhile, the difficulty of achieving hardware match between legitimate users will be also increased. Fortunately, all those hardware parameter mismatch tolerances are in the controllable range of commercial products. Practically, a tunable dispersion compensator (TeraXion, TDCMX) with a dispersion resolution of ~5 ps/nm, an electrically tunable optical delay line with a delay time resolution of ~1 ps, and an FSR tunable MZI (Kylia, WT-MINT) with

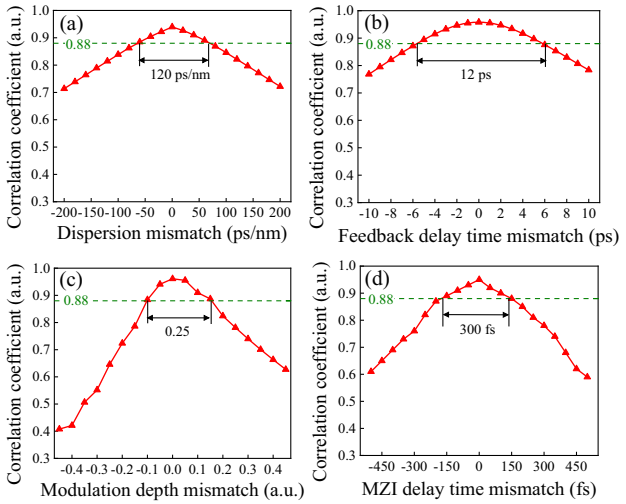

Fig. 8. Correlation coefficient at C and D versus (a) dispersion mismatch; (b) feedback delay time mismatch; (c) PM modulation depth mismatch; (d) MZI interference delay time mismatch.

a voltage-controlled interference delay time resolution of ~15 fs are all commercially available to control the hardware mismatch.

Based on the key parameter mismatch tolerances, the hardware key space enhancement can be evaluated when compared with that of using a solitary DFB laser as the response chaotic source, which provides a laser inner parameter key space of $\sim 2^{45}$ in this scheme. Assuming that a tunable dispersion compensator with a maximum dispersion tuning range of ±3000 ps/nm, a tunable MZI with a free spectral range of 3.33 GHz to infinite, and a feedback loop delay time of 100 ns are employed in the setup, a total hardware key space enhancement of $\sim 2^{32}$ can be obtained according to the previous reported key space analysis method [48,49]. By enlarging the delay time in the phase feedback loop and cascading additional dispersion elements, a further expanded hardware key space can be expected. It is extremely difficult for a malicious eavesdropper to perform brute-force attacks by searching through all possible combinations of the hardware key parameters, which provides enhanced hardware security for the private chaotic scrambling signal and thus guarantees the security of the key distribution simultaneously. Compared with previous optical chaos key distribution schemes based on distilling correlated random bits from driving-response induced synchronized chaos [31–33], the security of this scheme can be improved in terms of significantly reduced driving-response cross-correlation, expanded hardware key space with an aggregated key space of $\sim 2^{77}$, and more importantly, supporting temporal concealment of the secret key and scrambling of the phase distribution by a private chaotic signal. Accordingly, the hardware complexity is inevitably increased since there is always a tradeoff between complexity and security. It has been demonstrated that all the related chaotic signal processing can be implemented using commercial hardware components with controllable complexity. Although two wavelengths are employed for the proof-of-principle demonstration of secure key distribution instead of establishing two individual fiber transmission links with the third-party common driving source, the wavelength channel for distributing the noise-driving signal can be potentially replaced by the noise channel located between two transmission channels in a multi-channel environment or reusing the normal digital signal transmission channel as the driving channel to save valuable wavelength resources in future.

C. Performance of the Classical Secure Key Distribution

After achieving chaos synchronization, private chaotic phase scrambling and temporal steganographic transmission are applied to demonstrate the high-speed secure key distribution. Figures 9(a)–9(j) show the typical measured waveforms and corresponding eye diagrams for the temporal stealthy and private phase scrambled key signals in different scenarios. As depicted in Figs. 9(a) and 9(b), in the case of without chaotic phase scrambling, the phase modulated digital key sequence can be directly demodulated using the corresponding MZI. After the demodulation, the digital key signal with non-return-to-zero (NRZ) data format and a clear eye diagram of 10 Gb/s can be easily obtained without any security against eavesdropping. In contrast to the Figs. 9(a) and 9(b), when the digital key sequence is phase scrambled by the synchronized

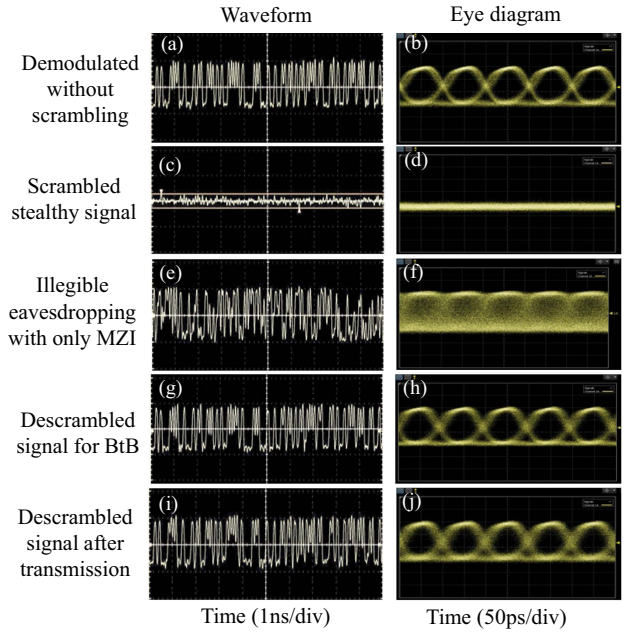

Fig. 9. Waveforms and eye diagrams for (a), (b) the demodulated key without scrambling, (c), (d) the scrambled signal without demodulation, (e), (f) the illegible eavesdropped signal using only an MZI, (g), (h) the properly descrambled key in BtB case, and (i), (j) the descrambled signal after transmission.

private chaotic signal and temporally concealed into the background noise in the time domain, the measured waveform and corresponding eye diagram exhibit as a noise, making an eavesdropper unaware of the existence of the private digital key sequence in the transmission channel and preventing the eavesdropping attack. In the worst-case scenario, even if an eavesdropper intercepts the chaotic scrambled signal in the transmission link and attempts to extract the private key sequence using a matched MZI, only a disordered random pattern will be obtained due to the absence of proper private chaotic phase descrambling, utterly unrelated to the original private key sequence, as illustrated in Fig. 9(e). Accordingly, the eye diagram after the MZI demodulation is completely closed, indicating that the proposed key distribution scheme is strongly secure against a sophisticated eavesdropper's attack with well-equipped demodulation components, which is shown in Fig. 9(f). Therefore, the security of such a classical key distribution scheme is sufficiently guaranteed by the dual-level of temporal steganography without awareness and private chaotic phase scrambling without being cracked. The temporal steganography contributes to enhancing the security of stand-alone chaotic phase scrambling.

On the contrary, for a legitimate user (Bob) that owns not only the demodulation components but also the matched chaotic response source to perform first the private chaotic phase descrambling and then the digital key demodulation, the private key can be successfully retrieved with correct bit patterns and a clear eye diagram, as depicted in Figs. 9(g) and 9(h). Figure 9(i) shows the received private key sequence after 40 km transmission, which is still well preserved and distributed to Bob. The corresponding eye diagram in Fig. 9(j) is

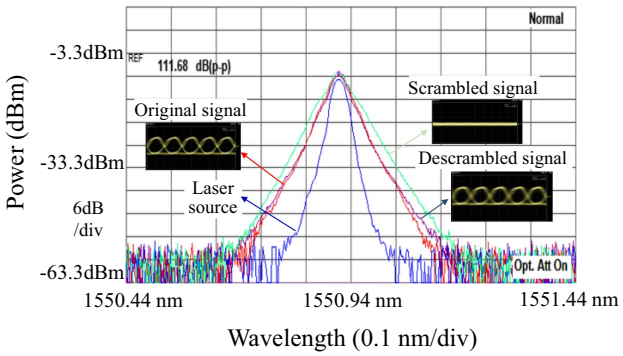

Fig. 10. Optical spectra for the original signal, chaotic phase scrambled signal, and descrambled signal, respectively.

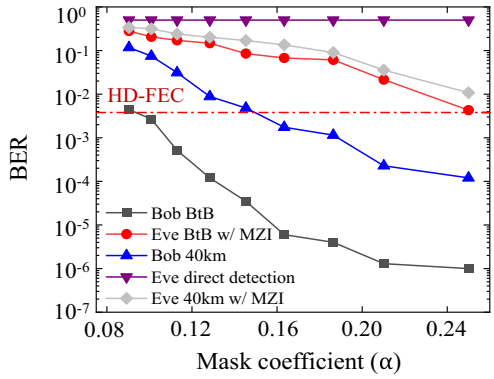

Fig. 11. BER performance versus mask coefficient for the legitimate user and an eavesdropper in the BtB and transmission scenarios.

clearly open with negligible degradation compared with the case of back-to-back (BtB) in Fig. 9(h), which successfully demonstrates secure distribution of a high-speed 10 Gb/s private key over the classical optical fiber channel. One may note that the optical chaos key distribution process in this scheme exhibits an encrypted phase-shift-keying data transmission in the physical transmission layer, but more than that, it is essentially a combination of temporal concealment and phase scrambled secret key transmission for chaos protected key distribution with a true random digital key as a requisite.

Figure 10 shows the optical spectral evolution of the laser source (blue line), the original key modulated signal (red line), and the chaotic phase scrambled/descrambled signals (green and purple lines), respectively. Compared with the original key modulated signal, the implementation of chaotic phase scrambling causes the optical spectrum to be slightly expanded due to the phase modulation induced spectral broadening. After performing chaotic phase scrambling via utilizing the synchronized private chaotic signal generated by the matched chaotic response source, the legitimate user is able to erase the imposed chaotic phase, leaving alone the phase shift keying modulation of the digital key sequence. The corresponding optical spectrum after descrambling is compressed back and resembles the spectrum of the original key modulated signal, indicating that the digital key has been successfully extracted and distributed to Bob.

To evaluate the secure key distribution performance, Fig. 11 depicts the measured BER versus the mask coefficient (α) for different scenarios. The black line represents the measured BER performance of the descrambled key sequence for the legitimate user Bob in the BtB case, where the BER decreases with the increasing of the mask coefficient. It is clear that the BER is always lower than the HD-FEC limit of 3.8×10^{-3} when the mask coefficient is larger than 0.09. The BER performance of the descrambled key sequence after 40 km transmission is shown as the blue line, which exhibits a similar tendency to the BtB case, but the mask coefficient is shifted to be larger than 0.15 to enable the BER to be lower than the HD-FEC limit. Therefore, there is a lower bound limit for the mask coefficient to guarantee the key distribution performance. As for a malicious eavesdropper with simple direct detection to intercept the temporal stealthy and chaotic scrambled secure key sequence, the measured BER stably keeps as 0.5, which is clearly shown as the purple line. In the case of a malicious attack by employing an MZI for direct phase demodulation, the measured BER is always larger than the HD-FEC limit when the mask coefficient is less than 0.25 for both the BtB and transmission cases. Even if Eve intercepts the driving signal and applies it for chaotic phase descrambling, the obtained BER is still not lower than the HD-FEC limit thanks to the low correlation between the driving and private response signals induced by the PRCM hardware. However, when the mask coefficient exceeds the upper bound limit of 0.25, the secure key sequence will emerge from the chaotic scrambling signal, and the measured BER is lower than the HD-FEC limit. Hence, the key distribution system will become unsecure when the mask coefficient is too large. In other words, for a direct detection attack, the private chaotic scrambling technique alone can still guarantee the system security in the absence of the temporal concealing process. But for an advanced phase demodulation attack, the security provided by pure chaotic phase scrambling would be threatened without the temporal concealing process. It becomes essential to simultaneously implement temporal steganographic transmission and private chaotic phase scrambling for secure key distribution against different attacks. To guarantee the BER performance and security of key distribution against eavesdropping, the mask efficient should be controlled in the range of 0.15–0.25 for the transmission scenario. Generalized key reconciliation and privacy enhancement algorithms can be further applied for post-processing of the distributed key sequence [50–52].

In addition, the effects of $PM_{3,4}$ phase modulation depth mismatch and synchronization delay time mismatch between the chaos synchronization and SKD channels on the BER performances are also measured, as depicted in Figs. 12(a) and 12(b). It is evident that both the PM modulation depth mismatch and channel delay time mismatch lead to the deterioration of BER performance. A lower mask coefficient causes reduced hardware parameter mismatch tolerances. A PM modulation depth mismatch of $\sim \pm 3$ dB and channel synchronization delay time mismatch tolerance of $\sim \pm 25$ ps could be tolerated for the lower bound limit of the mask coefficient to guarantee the BER to be lower than HD-FEC threshold. Increasing the mask coefficient upon the upper bound limit

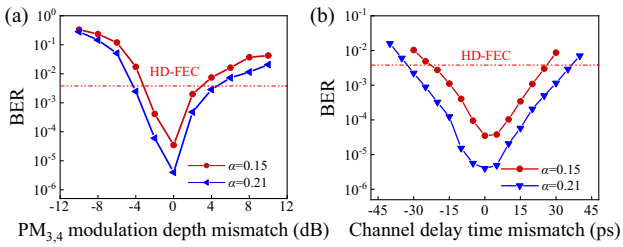

Fig. 12. BER performances versus (a) the PM modulation depth mismatch and (b) the channel synchronization delay time mismatch.

would lead to much relaxed mismatch tolerances, which can be properly handled by variable attenuators and tunable optical delay lines in the setup. The sensitive synchronization delay time of the chaos descrambling channel with respect to the SKD channel makes it impossible for an eavesdropper to descramble the SKD signal without proper time synchronization even if the private chaotic descrambling signal is available, let alone just by intercepting the driving signal.

Finally, as one of the key indicators for secure key distribution, it should be pointed out that the net secret key rate in the current system is closely related to the attack detection methods and mask coefficient employed. For a conventional power detection attack, the Eve cannot obtain any confidential phase information after 40 km transmission, resulting in a upper bound of a secret key rate of 10 Gb/s. However, for a sophisticated Eve's attack with MZI demodulation, considering that there is information leakage to Eve when varying the mask coefficient, the net secret key rate should be calculated by (10 Gb/s) × [MI(Legal)−MI(Illegal)], where MI represents the mutual information. For a mask coefficient of 0.15, the resultant net secret key rate is around 7.3 Gb/s and 6.6 Gb/s for BtB and 40 km transmission. A higher mask coefficient would induce larger information leakage and lower net secret key rate. It should also be noted that the achievable upper bound secret key rate is mainly limited by the bit rate of the source key generator and the PM modulation bandwidth, as well as the chaos bandwidth of the private scrambling signal. Further improvement of the upper bound secret key rate up to 40 Gb/s can be anticipated by employing a much faster key generator, a broadband $LiNbO_3$ PM, and a wideband chaotic entropy source, whose chaos bandwidth should be no less than the secret key rate to ensure efficient masking of the secret key and avoid filtering attack. It is also desirable to achieve long-distance key distribution for not only metropolitan-area networks but also backbone network-oriented secure communications with up to thousands of kilometers, in which case the primary challenges are establishing high-quality chaos synchronization after the long-reach transmission link and high-fidelity transmission of the phase scrambled secret key signal. Since the long-distance transmission would inevitably introduce fiber channel impairments arising from the chromatic dispersion, fiber nonlinearity, and accumulated amplified spontaneous emission noise, it is essential to optimize the transmission link by precisely compensating the chromatic dispersion and employing hybrid EDFA and distributed fiber Raman amplifiers to achieve long-distance chaos synchronization and key distribution [53], which remains for our future exploration.

4. CONCLUSION

In summary, we propose and experimentally demonstrate a new way for high-speed physical layer key distribution based on temporal steganography and chaotic phase scrambling over the classical optical fiber channel. A record high secret key rate of 10 Gb/s over 40 km single mode fiber is successfully achieved in the experiment. The security of the proposed key distribution scheme is double guaranteed by the first layer of temporal steganographic transmission to avoid the awareness of an eavesdropper and the second layer of bit-by-bit chaotic random phase scrambling by synchronous private chaotic signals. A common noise-driving induced synchronization scheme is adopted to generate the synchronized private chaotic scrambling and descrambling signals between the legitimate user's sides. Based on the injection of a chaotic signal output from an open-loop noise-driven semiconductor laser into an electro-optic phase feedback loop, an electro-optic hybrid chaotic hardware response source is established to simultaneously suppress the high residual driving-response correlation and expand the hardware key space, which further contributes to greatly enhancing the security for key distribution. The proposed approach may provide a new strategy for achieving high-speed classical key distribution based on advanced chaotic signal processing and optical steganography using the standard single mode fiber channel and commercially mature components. It also has great potential to be combined with digital cryptography for applications in future high-speed secure communication systems.

Funding. National Key Research and Development Program of China (2023YFB2906000); National Natural Science Foundation of China (62004047, 62375055, U2001601, U22A2087); Guangdong Basic and Applied Basic Research Foundation (2023B1515020088); Guangdong Introducing Innovative and Entrepreneurial Teams of "The Pearl River Talent Recruitment Program" (2019ZT08X340).

Disclosures. The authors declare no conflicts of interest.

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

REFERENCES

1. X. Zhang, H. Ji, M. Luo, *et al.*, "3.61 Pbit/s S, C, and L-band transmission with 19-core single-mode fiber," IEEE Photon. Technol. Lett. **35**, 830–833 (2023).
2. B. J. Puttnam, G. Rademacher, and R. S. Luís, "Space-division multiplexing for optical fiber communications," Optica **8**, 1186–1203 (2021).
3. Y. Gong, R. Kumar, A. Wonfor, *et al.*, "Secure optical communication using a quantum alarm," Light Sci. Appl. **9**, 170 (2020).
4. N. S. Kapov, M. Furdek, S. Zsigmond, *et al.*, "Physical-layer security in evolving optical networks," IEEE Commun. Mag. **54**, 110–117 (2016).
5. S. Rothe, N. Koukourakis, H. Radner, *et al.*, "Physical layer security in multimode fiber optical networks," Sci. Rep. **10**, 2740 (2020).

6. M. Fok, Z. Wang, Y. Deng, *et al.*, "Optical layer security in fiber-optic networks," IEEE Trans. Inf. Forensics Security **6**, 725–736 (2011).
7. C. E. Shannon, "Communication theory of secrecy systems," Bell Syst. Tech. J. **28**, 656–715 (1949).
8. M. Iqbal, L. Velasco, N. Costa, *et al.*, "LPsec: a fast and secure cryptographic system for optical connections," J. Opt. Commun. Netw. **14**, 278–288 (2022).
9. T. Qiu, W. Shao, L. Deng, *et al.*, "Secure key distribution based on the polarization reciprocity of fiber and a coherent reception architecture," Opt. Lett. **48**, 3547–3550 (2023).
10. L. Zhang, X. Huang, Z. Chai, *et al.*, "Unidirectional physical layer secure key distribution in a fiber channel assisted by neural networks," Opt. Lett. **47**, 4263–4266 (2022).
11. S. Aftergood, "The darkening web: the war for cyberspace," Nature **547**, 30–31 (2017).
12. K. A. G. Fisher, A. Broadbent, L. K. Shalm, *et al.*, "Quantum computing on encrypted data," Nat. Commun. **5**, 3074 (2014).
13. E. Diamanti, H. K. Lo, B. Qi, *et al.*, "Practical challenges in quantum key distribution," npj Quantum Inf. **2**, 16025 (2016).
14. F. Cavaliere, E. Prati, L. Poti, *et al.*, "Secure quantum communication technologies and systems: from labs to markets," Quantum Rep. **2**, 80–106 (2020).
15. J. Scheuer and A. Yariv, "Giant fiber lasers: a new paradigm for secure key distribution," Phys. Rev. Lett. **97**, 140502 (2006).
16. A. E. Taher, O. Kotlicki, P. Harper, *et al.*, "Secure key distribution over a 500 km long link using a Raman ultra-long fiber laser," Laser Photon. Rev. **8**, 436–442 (2014).
17. D. B. Lev and J. Scheuer, "Enhanced key-establishing rates and efficiencies in fiber laser key distribution systems," Phys. Lett. A **373**, 1101–4296 (2009).
18. A. Tonello, A. Barthelemy, K. Krupa, *et al.*, "Secret key exchange in ultralong lasers by radio frequency spectrum coding," Light Sci. Appl. **4**, e276 (2015).
19. A. Zadok, J. Scheuer, J. Sendowski, *et al.*, "Secure key generation using an ultra-long fiber laser: transient analysis and experiment," Opt. Express **16**, 16680–16690 (2008).
20. K. Kravtsov, Z. X. Wang, W. Trappe, *et al.*, "Physical layer secret key generation for fiber-optical networks," Opt. Express **21**, 23756–23771 (2013).
21. I. U. Zaman, A. B. Lopez, M. A. A. Faruque, *et al.*, "Physical layer cryptographic key generation by exploiting PMD of an optical fiber link," J. Lightwave Technol. **36**, 5903–5911 (2018).
22. A. A. E. Hajomer, L. Zhang, X. Yang, *et al.*, "284.8-Mb/s physical-layer cryptographic key generation and distribution in fiber networks," J. Lightwave Technol. **39**, 1595–1601 (2021).
23. W. Shao, M. Cheng, L. Deng, *et al.*, "High-speed secure key distribution using local polarization modulation driven by optical chaos in reciprocal fiber channel," Opt. Lett. **46**, 5910–5913 (2021).
24. M. Sciamanna and K. A. Shore, "Physics and applications of laser diode chaos," Nat. Photonics **9**, 151–162 (2015).
25. A. Argyris, E. Grivas, M. Hamacher, *et al.*, "Chaos-on-a-chip secures data transmission in optical fiber links," Opt. Express **18**, 5188–5198 (2010).
26. A. Argyris, D. Syvridis, L. Larger, *et al.*, "Chaos-based communications at high bit rates using commercial fibre-optic links," Nature **438**, 343–346 (2005).
27. I. Kanter, M. Butkovski, Y. Peleg, *et al.*, *et al.*, "Synchronization of random bit generators based on coupled chaotic lasers and application to cryptography," Opt. Express **18**, 18292–18302 (2010).
28. X. Porte, M. C. Soriano, D. Brunner, *et al.*, "Bidirectional private key exchange using delay-coupled semiconductor lasers," Opt. Lett. **41**, 2871–2874 (2016).
29. C. Xue, N. Jiang, Y. Lv, *et al.*, "Secure key distribution based on dynamic chaos synchronization of cascaded semiconductor laser systems," IEEE Trans. Commun. **65**, 312–319 (2017).
30. N. Jiang, C. P. Xue, D. Liu, *et al.*, "Secure key distribution based on chaos synchronization of VCSELs subject to symmetric random-polarization optical injection," Opt. Lett. **42**, 1055–1058 (2017).
31. L. Wang, M. Chao, A. Wang, *et al.*, "High-speed physical key distribution based on dispersion-shift-keying chaos synchronization in commonly driven semiconductor lasers without external feedback," Opt. Express **28**, 37919–37935 (2020).
32. H. Gao, A. Wang, L. Wang, *et al.*, "0.75 Gbit/s high-speed classical key distribution with mode-shift keying chaos synchronization of Fabry-Perot lasers," Light Sci. Appl. **10**, 172 (2021).
33. Z. Gao, Z. Ma, S. Wu, *et al.*, "Physical secure key distribution based on chaotic self-carrier phase modulation and time-delayed shift keying of synchronized optical chaos," Opt. Express **30**, 23953–23966 (2022).
34. T. Sasaki, I. Kakesu, Y. Mitsui, *et al.*, "Common-signal-induced synchronization in photonic integrated circuits and its application to secure key distribution," Opt. Express **25**, 26029–26044 (2017).
35. H. Koizumi, S. Morikatsu, H. Aida, *et al.*, "Information-theoretic secure key distribution based on common random-signal induced synchronization in unidirectionally-coupled cascades of semiconductor lasers," Opt. Express **21**, 17869–17893 (2013).
36. K. Yoshimura, J. Muramatsu, P. Davis, *et al.*, "Secure key distribution using correlated randomness in lasers driven by common random light," Phys. Rev. Lett. **108**, 070602 (2012).
37. T. Yamamoto, I. Oowada, H. Yip, *et al.*, "Common-chaotic-signal induced synchronization in semiconductor lasers," Opt. Express **15**, 3974–3980 (2007).
38. F. Bohm, S. Sahakian, A. Dooms, *et al.*, "Stable high-speed encryption key distribution via synchronization of chaotic optoelectronic oscillators," Phys. Rev. Appl. **13**, 064014 (2020).
39. S. Liu, N. Jiang, Y. Zhang, *et al.*, "Secure key distribution based on hybrid chaos synchronization between semiconductor lasers subject to dual injections," Opt. Express **30**, 32366–32380 (2022).
40. Z. Zhao, M. Cheng, C. Luo, *et al.*, "Semiconductor-laser-based hybrid chaos source and its application in secure key distribution," Opt. Lett. **44**, 2605–2608 (2019).
41. Z. Gao, S. Wu, Z. Deng, *et al.*, "Private correlated random bit generation based on synchronized wideband physical entropy sources with hybrid electro-optic nonlinear transformation," Opt. Lett. **47**, 3788–3791 (2022).
42. A. Zhao, N. Jiang, Y. Wang, *et al.*, "Correlated random bit generation based on common-signal-induced synchronization of wideband complex physical entropy sources," Opt. Lett. **44**, 5957–5960 (2019).
43. N. Jiang, A. Zhao, C. Xue, *et al.*, "Physical secure optical communication based on private chaotic spectral phase encryption/decryption," Opt. Lett. **44**, 1536–1539 (2019).
44. Z. Gao, Q. Wu, L. Liao, *et al.*, "Experimental demonstration of synchronous privacy enhanced chaotic temporal phase en/decryption for high speed secure optical communication," Opt. Express **30**, 31209–31219 (2022).
45. A. Zhao, N. Jiang, S. Liu, *et al.*, "Physical layer encryption for WDM optical communication systems using private chaotic phase scrambling," J. Lightwave Technol. **39**, 2288–2295 (2021).
46. B. Wu, Z. Wang, Y. Tian, *et al.*, "Optical steganography based on amplified spontaneous emission noise," Opt. Express **21**, 2065–2071 (2013).
47. Q. Cai, P. Li, Y. Shi, *et al.*, "Tbps parallel random number generation based on a single quarter-wavelength-shifted DFB laser," Opt. Laser Technol. **162**, 109273 (2023).
48. D. Wang, L. Wang, Y. Guo, *et al.*, "Key space enhancement of optical chaos secure communication: chirped FBG feedback semiconductor laser," Opt. Express **27**, 3065–3073 (2019).
49. C. Huang, X. Gao, S. Wu, *et al.*, "Key space enhanced correlated random bit generation based on synchronized electro-optic self-feedback loops with Mach–Zehnder modulators," Photonics **9**, 952 (2022).
50. J. M. Mateo, D. Elkouss, and V. Martin, "Key reconciliation for high performance quantum key distribution," Sci Rep. **3**, 1576 (2013).
51. S. Chen, L. Zhang, W. Hu, *et al.*, "Efficient post-processing for physical-layer secure key distribution in fiber," IEEE Photon. Technol. Lett. **33**, 325–328 (2021).
52. C. Bennett, G. Brassard, and U. M. Maurer, "Generalized privacy amplication," IEEE Trans. Inf. Theory **41**, 1915–1923 (1995).
53. L. Wang, J. Wang, Y. Wu, *et al.*, "Chaos synchronization of semiconductor lasers over 1040-km fiber relay transmission with hybrid amplification," Photon. Res. **11**, 953–960 (2023).