Ultrafast Secure Key Distribution Based on Random DNA Coding and Electro-Optic Chaos Synchronization

Xue, Chenpeng; Wan, Hongdan; Gu, Ping; Jiang, Ning; Hong, Yanhua; Zhang, Zuxing

IEEE Journal of Quantum Electronics

DOI: 10.1109/JQE.2021.3139711

Published: 01/02/2022

Peer reviewed version

Cyswllt i'r cyhoeddiad / Link to publication

Dyfyniad o’r fersiwn a gyhoeddwyd / Citation for published version (APA):

Hawliau Cyffredinol / General rights
Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

• Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
• You may not further distribute the material or use it for any profit-making activity or commercial gain
• You may freely distribute the URL identifying the publication in the public portal

Take down policy
If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.
Ultrafast Secure Key Distribution Based on Random DNA Coding and Electro-Optic Chaos Synchronization

Chenpeng Xue, Hongdan Wan, Ping Gu, Ning Jiang, Yanhua Hong, and Zuxing Zhang

Abstract—We propose and numerically demonstrate an ultrafast secure key distribution based on random DNA coding and the chaos synchronization in two identical electro-optic oscillators (EO) with common injection. High-quality synchronization between the responses of EOs with extremely sensitivity to the mismatching of time delay and phase bias is observed. It is noted that the random DNA coding and the delay DNA-XOR in the post-processing can greatly amplify the randomness of the synchronized sequences acquired by symmetrically dual-threshold sampling the correlated physical entropies, and enhance the security of key distribution by providing additional encryption. According to our study, high rate key distribution of over 10 Gb/s can be fulfilled with a good consistency, which can be used for the commercial communication networks.

Index Terms—Secure key distribution, Random DNA coding, chaos synchronization, electro-optic chaos.

I. INTRODUCTION

Private and secure communication has been of fundamental importance as it plays a vital role in all areas of military, economy, and social life. There is an agreement that the communicating parties have to hold a common secure key known only to themselves to ensure the security. In general, the secure key distribution (SKD) schemes can be classified into two categories, the mathematical algorithm-based key distribution, and the physical phenomenon-based key distribution. The former is based on the computational intractability of certain mathematical functions, therefore may suffer from exhaustive attack with the advancing in computational ability, whereas the latter does not dependent on the computational power of computers. Inspired by this, many key distribution schemes based on abundant nonlinear optical phenomena and principles have been proposed, such as quantum key distribution [1, 2], SKD utilizing giant fiber laser [3-5], SKD based on the optical chaos [6, 7], or broadband optical noise [8].

Among them, the SKD based on the optical chaos in semiconductor laser (SL) has been of increasing interest, since it can afford high-speed up to Gb/s, which can be used for high-rate secure digital transmission with the one-time-pad cryptographic protocol [8-10]. The fundamental of the key distribution protocol is to create synchronized random bit sequences by symmetrically sampling correlated entropies privately [11]. As the physical random entropies of the SKD should be privately synchronized for the purpose of security, the common-injection synchronization mechanism is well-respected [12]. Yoshimura et al. proposed SKD using correlated chaotic signals in lasers driven by common random light and discussed its information theoretic security with the “bounded observability” [13, 14]. Li et al. proposed the correlated random bit generation using chaotic SLs under unidirectional common optical injection [15]. Zhao et al. proposed a synchronized random bit generation technique based on analog-digital hybrid electro-optic chaos where the digital signal is transmitted as the seed to achieved chaos synchronization [16]. Wang et al., proposed a 2.5 Gb/s real-time correlated random bit generation based on synchronized chaos induced by a common laser with dispersive feedback [17]. Huang et al., propose a SKD up to 1.34 Gb/s based on polarization-keying chaos synchronization in quantum dot spin-polarized vertical-cavity surface-emitting lasers without any external feedback [18]. Very recently, Gao et al., experimentally demonstrate a 0.75 Gb/s SKD based on mode-shift keying chaos synchronization [19]. In our previous work, we have introduced a SKD based on correlated random bit generators with the dynamic post-processing [20], and the correlated random bit generation based on common-signal-induced synchronization of wideband physical entropy sources [21]. However, limit by the entropy properties and distribution protocol, the key distribution rate of the proposed schemes is in the magnitude of Gb/s, and there is still a critical need for higher rate.

Moreover, though the synchronized chaos presents highly
unpredictable characteristics and bandwidth, post-processing technologies such as self-heterodyne, delay bitwise XOR, high order digital derivation in the analog and digital domain are still adopted widely to amplify the randomness of the synchronized sequence [16, 22-24]. In this work, we present an alternate way to enhance the key distribution rate by employing more powerful post-processing. DNA computing has the characteristics of massive parallelism, huge storage, ultra-low power consumption, and is widely used in encryption systems [25-27]. Herein, we propose and numerically demonstrate the ultrafast SKD based on random DNA coding and chaos synchronization in the electro-optic oscillators (EO) driven by a common chaotic signal. The common chaotic signal is generated in a SL with chirped fiber Bragg grating (CFBG) feedback and two identical EOs are used as the nonlinear scramblers. The paper is organized as follows: the scheme and theoretical model are described in Section II; followed by the numerical simulation results in Section III; finally, we summarize the results in Section IV.

II. SCHEME AND SYSTEM MODEL

Fig. 1 shows the schematic configuration of the proposed SKD scheme. The chaotic output of a SL with CFBG feedback is amplified by an EDFA and divided equally into two parts as the common injections for the EOs, which are composed with several elements: a continuous-wave SL, a Mach-Zehnder modulator (MZM), a fiber delay line (FDL), a photodiode (PD) and a radio-frequency amplifier (RFA). The driving signal of MZM is the mixture of the feedback electrical signal and the injection signal after photoelectric conversion. The output of the EO is used for the self-heterodyne, where it is detected by the PD and IPD with a precise FDL2 simultaneously, and the generated electrical signals are mixed by an electrical mixer as the correlated physical entropy. In the ADC module, the symmetric dual-threshold sampling is used to generate a synchronized binary sequence between Alice and Bob from the physical entropies. Then the initial binary sequence is encoded into DNA sequence according to a dynamic rule controlled by the DNA-key and the delay DNA-XOR is deployed [See the Table I and Table II]. Finally, the secure key is obtained by decoding the DNA-sequence with a certain rule, e.g., rule one.

The electronic bandwidth of the feedback loop in the EOs in approximation results from two cascaded linear first-order low-pass and high-pass filters, with low and high cutoff frequencies \( f_0 \) and \( f_0 \), respectively. We consider \( x=\pi V/(2V_d) \) as the dimensionless variable describing the system, where \( V \) and \( V_d \) are the intrinsic electrical voltage and radio frequency half-wave voltage for the MZM respectively, its dynamics can be modeled by the following integro-differential delayed equation [28-31]:

\[
\begin{align*}
    \frac{dx_{1,2}}{dt} &+ \int_0^t \phi(s) ds \\
    &= \beta_{1,2} \cos\left[\int_0^t (x_{1,2}(t-T_D) + x_{1,2} + \phi_{1,2})\right]
\end{align*}
\]

where the subscripts 1 and 2 represent EO1 and EO2 respectively. For the phase bias, \( \theta=1/(2\pi f_0) \) and \( \tau=1/(2\pi f_0) \) are the low and high cut-off response times of the electronic feedback, respectively.

\[
\beta=\pi GP/(2V_d)
\]

descrip the feedback strength. \( \phi \) is defined as the phase bias. \( P \) and \( G \) are the power of the light detected by the PD and the gain of the RFA respectively. \( V_{\text{dc}} \) is the dc half-wave voltage. \( T_D \) is the delay time of the FDL1 in EO. Similarly, the injection signal is defined as \( x_{1,2}=\pi GP_{in}/(2V_d) \), where \( P_{in} \) is the power of injection light.


<table>
<thead>
<tr>
<th>TABLE I</th>
<th>DNA ENCODING AND DECODING RULES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Binary</td>
<td>1</td>
</tr>
<tr>
<td>00</td>
<td>A</td>
</tr>
<tr>
<td>01</td>
<td>C</td>
</tr>
<tr>
<td>10</td>
<td>G</td>
</tr>
<tr>
<td>11</td>
<td>T</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>TABLE II</th>
<th>DNA XOR OPERATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>XOR</td>
<td>A</td>
</tr>
<tr>
<td>A</td>
<td>A</td>
</tr>
<tr>
<td>G</td>
<td>G</td>
</tr>
<tr>
<td>C</td>
<td>C</td>
</tr>
<tr>
<td>T</td>
<td>T</td>
</tr>
</tbody>
</table>

The modifying Lange-Kobayashi rate equations are adopted to model the evolutions of the complex amplitude electric field \( E \) and the carrier number \( N \) in the SL with CFBG feedback [32-34], which can be written as
\[
\frac{dE}{dt} = (1 + i\alpha) \left( \frac{g[N(t) - N_0]}{1 + e|E(t)|^2} - \gamma_e \right) E(t) + k_I \int_{-\infty}^{t} h(t - T') E(t' - \tau_e) dt',
\]
\[
\frac{dN}{dt} = \frac{I}{q} \gamma_e N(t) - \frac{g[N(t) - N_0]}{1 + e|E(t)|^2} |E(t)|^2
\]

where, \(\alpha\) is the linewidth enhancement factor, \(\gamma_e\) is the photon decay rate, \(\gamma_p\) is the carrier decay rate, \(g\) is the gain saturation coefficient, \(N_0\) is the transparent carrier number, \(I\) is the pump current and \(q\) is the electron charge. \(\tau_e\) and \(k_I\) are the time delay and strength of optical feedback, respectively. The second term in the right side of (2) represents the CFBG feedback. \(h(t)\) specifies the impulse response of the CFBG with respect to the reflection frequency response \(H(\omega)\). Therefore, the CFBG feedback can be calculated by the inverse Fourier transform of \(H(\omega)\). FT\{\} denotes the Fourier transform. To simulate the CFBG, the piecewise-uniform approach is utilized \([35, 36]\). Frankly, the CFBG is equally discretized into short sections that can be approximated to the uniform gratings, of which the transfer matrix can allow for the calculation of the CFBG by simply cascading the transfer matrices appropriate to each discretization.

In our simulation, \(\tau_e=3\) ns, \(k_I=20\) ns\(^{-1}\) and \(I=30.87\) mA, the intrinsic parameter values of SL are set as the typical values reported in \([37]\), \(\theta_e=5\) \(\mu_s\), \(\tau_{\text{ps}}=5\) ps, \(T_{\text{ps}}=5\) fs, \(\alpha = 5, \gamma_p = 0.5\) ps\(^{-1}\), \(\gamma_e = 0.5\) ns\(^{-1}\), \(g = 1.5 \times 10^8\) ps\(^{-1}\), \(N_0 = 1.5 \times 10^6\), \(e = 5 \times 10^{-7}\). The CFBG parameters are set in line with \([36]\), where the chirp factor \(C=0.02\) nm/cm, the effective refractive index \(n_{\text{eff}}=1.46\), the average index change \(\delta_{\text{eff}}=5 \times 10^{-5}\), the grating length \(L=10\) cm and the center wavelength 1550 nm. The integral time \(T\) for calculating dispersive feedback is set as 20.48 ns. Neglecting the dc component, the \(x_{\text{inj}}\) is mathematically described as

\[
x_{\text{inj}} = \mu \cdot \text{Nor} \left( \left| E(t) \right| - \left< \left| E(t) \right| \right> \right)
\]

where \(\text{Nor}\) denotes the normalization and \(<\cdot>\) denotes the time averaging. \(\mu\) defined as the injection factor is used to quantitatively describe the injection strength.

### III. RESULTS AND ANALYSES

#### A. Chaos synchronization

Fig. 2 presents synchronization properties between the injection and responses of the OEs. As shown in Fig. 2 (a), with the parameters of \(\beta=2.5, \phi_e=2.1\) and \(\mu=6.75\), the two responses \(x_1\) and \(x_2\) present identical chaotic time series, which are significantly different from the injection \(x_{\text{inj}}\). Fig. 2 (b) and (c) corresponding to the power spectra of the injection and response also show significantly difference. For instance, the spectrum of the response witnesses a monotonically decreasing, whereas the injection holds a spectrum of which the energy focuses around the relaxation oscillation frequency of the SL [36]. Fig. 2 (d) and (e) are the cross-correlation plots between the responses, and between the injection and response, respectively. The cross-correlation coefficient (CC) is used to describe the synchronization quality quantitatively [12, 20, 38]. Clearly, \(x_1\) and \(x_2\) are highly synchronized with a CC ~ 1, while the \(x_{\text{inj}}\) and \(x_1\) are not synchronized (CC ~ 0.15). The weak cross-relation between the injection and response matches our expectation that the leakage of the common injection signal would present extremely little information of the response.

![Fig. 2. Cross-correlation properties, (a) the temporary waveforms with offset, (b) and (c) are the power spectra of the injection and response, respectively, (d) cross-correlation plots between the responses, and (e) cross-correlation plots between the injection and response.](image)

![Fig. 3. Cross-correlation between the chaos in the space of \(\beta\) and \(\mu\) with \(\phi=\pi/25\) (left column), and in the space of \(\beta\) and \(\phi\) with \(\mu=6.75\) (right column), (a) and (b) are for the synchronization between the responses of the OEs, (c) and (d) correspond to synchronization between the injection and response.](image)
work at stable state until \( \beta \) reaches 2.4 [See the inset figure in Fig. 3(a)]. With the injection of chaotic signal, the response output of the EO is chaotic signal regardless of the injection strength. When \( \mu \leq 4 \), the changing of the threshold of \( \beta \) for chaos synchronization presents a complicated trajectory with the increasing of \( \mu \) since it can influence the complexity of the response and present common driving effect simultaneously. When \( \mu > 4 \), with the increasing of \( \mu \), the threshold of \( \beta \) is increased generally as the common driving effect dominates the synchronization. Fig. 5 (b) presents the synchronization evolution between the responses in the space of \( \beta \) and \( \phi \) with \( \mu = 6.75 \). High-quality synchronization can be observed with \( \beta < 2.7 \), from which the cross-correlation witnesses a rapidly decline with the raise of \( \beta \). Moreover, the threshold of \( \beta \) for chaos synchronization hardly changes with \( \phi \). It can be inferred that with relatively large \( \mu \), the synchronization performance between the responses is significantly related to \( \beta \) rather than \( \phi \). The evolution of cross-correlation between injection and response versus \( \beta, \mu \) and \( \phi \) is also investigated. As shown in Fig. 3, (c), only when \( \mu \) and \( \beta \) are relatively small, e.g., less than 2.5, CC>0.4 can be observed. With the increasing of \( \mu \) or \( \beta \), the CC decreases quickly since increasing \( \mu \) or \( \beta \) can improve the modulation depth of the MZM and then enhance its nonlinear effect. Fig. 3 (d) shows the cross-correlation evolution versus \( \phi \) and \( \beta \). Different from the synchronization between the responses, the cross-correlation between the injection and response is related to \( \phi \). When \( \phi \) set around 0 or \( \pm 0.5 \pi \), relatively low CC is identified.

Next, the robustness of chaos synchronization between the responses to the parameter mismatch is investigated. Fig. 4 (a) and (b) present the synchronization performance versus \( \phi \) mismatch. Here, the phase bias of MZM in EO2 is set as \( \phi = -\pi/2 \), whereas that in the EO1 (\( \phi_1 \)) is changed. As the modulation hold a period of \( \pi \), the mismatching of \( \phi \) is studied in the range of \(-\pi/2 \) to \( \pi/2 \) with respect to \( \pi/25 \). When \( \mu < 2 \), the robustness of synchronization to the \( \phi \) mismatch is relatively poor. With the increasing of \( \mu \), the affordable range of \( \phi \) mismatch for synchronization widens slowly because of the strong driving effect. Moreover, as shown in Fig. 4(b), with the increasing of \( \beta \), the affordable range of \( \phi \) mismatch for synchronization decreases gradually. When \( \beta \) is over 2.7, the high-quality synchronization can not be achieved. Fig. 4(c) and (d) present the robustness of chaos synchronization to the time delay mismatch. When \( \mu < 1 \), the synchronization can be obtained in a relatively wide mismatching range from -15 ps to 15 ps. With the increasing of \( \mu \), it decreases first and reaches the minimum values at \( \mu = 4.5 \). Further increasing \( \mu \), the tolerable mismatch widens again. Fig. 4 (d) shows the influence of \( \beta \) on the robustness of chaos synchronization to time delay mismatch. When \( \beta < 1.5 \), time delay mismatching over 100 ps is still permitted for high quality synchronization. With the increasing of \( \beta \), the affordable mismatching range decreases rapidly and disappears when \( \beta \) reaches 2.7.

Though the time delay loop plays a key role in the privacy chaos synchronization, and the small mismatch can lead the significant synchronization decay, its existing demonstrates correlation around the feedback round trip time and its multiples, namely, the time delay signature (TDS). The TDS would also reduce the randomness of SKD, which is undesired. To characterize the TDS embedded in the time series, the well-known auto-correlation function (ACF) and delayed mutual information (DMI) are adopted [23]. The sizes of ACF and DMI peaks located around the lag time equaling to the delay time provide a relative quantitative measure of TDS. Fig. 5 (a) and (b) show the evolution of the TDS size versus \( \phi \) and \( \beta \) calculated by the ACF and DMI, respectively. It is clear that when \( \beta < 0.6 \), the response of EO is majorly dependent on the injection signal, and the suppression of the TDS (TDS is less than 0.1 in ACF and less than 0.005 in DMI) can be achieved easily. With the increasing of \( \beta \), the TDS suppression areas are separated by the “banded islands” in the direction of the \( \phi \) axis. It can be interpreted as that MZM with \( \phi \) around the multiple of \( \pi/2 \) can provide stronger nonlinear effect [See the right side in (1)], which would limit the generation of TDS. The periodical distribution of the “banded islands” with a period of \( \pi \) is because that the MZM modulation is the square of cosine function. Moreover, the width of TDS suppression area between adjacent “banded islands” firstly narrows with the
increase of $\beta$, and then it broadens again. This is because when $\beta$ is relatively small, with the increase of $\beta$, the oscillation introduced by the opto-electric feedback is enhanced, thereby amplifying the TDS. Due to the nonlinear modulation of the MZM, further increase of $\beta$ would also raise the complexity and randomness of signal, which can lead to a broadening of the TDS suppression area. It should be noted that the excessive $\beta$ would degrade the chaos synchronization between the responses of the EOs [See Fig. 3(a) and (b)].

B. The key distribution and security analysis

Even though the synchronized response shows wide bandwidth and unpredictability, the use of the self-heterodyne response output rather than the response output itself as the physical entropy of the random key is recommended [16, 18], since it has a more symmetrical probability density function (PDF) as presented in Fig. 6. It has been demonstrated that the asymmetric of the PDF has a negative influence on the random bit generation, which would also affect the SKD by limiting randomness, and security. The dual-threshold quantization method is adopted to generate the shared key. With this method, the outputs larger than the upper-threshold are quantized as bits “1” and those smaller than the lower-threshold are quantized as bits “0”, whereas those between the upper- and lower-thresholds are discarded. By exchange the location of discard bits through the public channel, a synchronized binary sequence is established between Alice and Bob. To enhance its randomness, the random DNA coding and delay DNA-XOR are adopted. Here, the random DNA coding is implemented according to a recycled 512-byte key with a resolution of 3 bits shared by the communication parties, and each 16 bits of the synchronized binary sequences is encoded according to a certain encoding rule selected by the DNA key. The decoded binary key from the final DNA sequence is tested by NIST 800-22 TESTs, which are the standard tests for randomness [38]. Table. III shows the test result of SKD with a sampling rate $f_s=20$ Gb/s (1000 samples of 1 Mbit sequences). According to the principle, at significance level of $a_{th} = 0.01$, the success proportion should be in the range of 0.994±0.0094392 and the composite P-value should be larger than 0.0001. As we can see in Table III, all of the 15 NIST tests are passed, which indicate that the generated secure key hold a good randomness.

To illustrate the superior performances of the random DNA coding in the randomness amplification, a comparison between the randomness test with and without random DNA coding in the post-processing versus the sampling $f_s$ is presented in Fig. 7. Without the random DNA coding, the median number passed the tests is 14 with $f_s \leq 12.5$ Gb/s, then it decays rapidly with the increasing of $f_s$. Moreover, that minimum number passed tests is no more than 13 when $f_s$ is over 5 Gb/s. With the random DNA coding, when $f_s \leq 25$ Gb/s, the median number passed the tests is 14 and the minimum number over 14 can be observed, except $f_s$ at 8.33 Gb/s and 25 Gb/s.

In addition to randomness of the key, the consistency of key between Alice and Bob has also been studied. Here, the BER defined as the ratio of different bits in the key between communication parities to the whole sequence is used to characterize the consistency. Fig. 8(a) shows the influence of the $\beta$ mismatch on the synchronization and BER performance. Clearly, high-quality synchronization can be maintained in the range of (-20%, 15%) due to the common driving. There is an evident asymmetry between the positive and negative
mismatch that negative mismatch can afford higher synchronization quality than that of the positive with common degree of mismatching. It can be inferred that with the increasing of $\beta$, the chaos synchronization becomes more sensitive to $\beta$ mismatch. For instance, when $\beta$ is set to 2.5, the tolerable mismatching range of $\beta$ for high-quality synchronization is from -9% to 5% [Not shown here]. The BER of SKD is calculated with different retained ratios $r$, which is defined as the whole probability of symbol ‘1’ and ‘0’ appear in the sampling. By adjusting the values of the thresholds of sampling, $r$ can be control with great precision. Moreover, the dual thresholds should be set to keep the probability of symbol ‘1’ roughly equaling to that of ‘0’. As shown in Fig. 8(a), the BER increases with the increasing of $\beta$ mismatch, since the synchronization performance is degraded. Fortunately, BER under the threshold of the hard-detection forward error correction (HD-FEC) with 7% redundancy ($3.8 \times 10^{-3}$) can be hold with a good robustness to the mismatch of $\beta$. With the decreasing of $r$, the robustness can be further enhanced. Due to the asymmetric evolution of chaos synchronization, the BER also presents a similar asymmetry with respect to the mismatch of $\beta$. Fig. 8(b) shows the performance of SKD and synchronization as a function of $\mu$ mismatch. High-quality synchronization can be hold with the mismatch range of -10% to 11%. The small asymmetric also infers that the chaos synchronization can be more sensitive to the $\mu$ mismatch by decreasing the injection strength. Moreover, similar to the case of $\beta$ mismatch, the BER also degrades itself with the increasing of $\mu$ mismatch. Fig. 8 (c) and (d) present the chaos synchronization and BER performance versus the $\phi$ and $T_D$ mismatch respectively. Clearly, the BER properties and synchronization degrade with the increasing of the mismatch. Furthermore, the influence of the mismatch of the electronic bandwidth in the EOs on the SKD properties is also studied. As shown in Fig. 8(e), with the increasing of the mismatching of $\tau$, the synchronization properties would degrade and BER would increase, and high quality synchronization can be hold in the $\tau$ mismatch range of -20% to 30%. It is noted that both BER and chaos synchronization are more sensitive to the $\phi$ and $T_D$ mismatches than those of $\beta$, $\mu$ and $\tau$. By adjusting $r$, BER can also be optimized at the expense of the rate reduction of SKD. Therefore, there is a trade-off between the distributing rate and the consistency of SKD to some extent.

Finally, the rate and security of SKD is discussion. As the reduction of the distributing rate majorly comes from the dual-threshold sampling, the rate of SKD can be estimated as $r f_s$ roughly. Therefore, with $r=0.6$, the maximum rate of the proposed SKD is about 12 Gb/s. However, there will be inevitably disagreements on the discarded samples between Alice and Bob in the processing of dual-threshold sampling, and the actual retain ratio defined as $r_{act}$ is less than $r$ slightly. Here, with proportion of $p=r_{act}/r$, the actual SKD rate can be described by $p \cdot r f_s$. For instance, $p=1$ indicates no reduction of the SKD rate, while $p=0$ means that no secure key is generated. As shown in Fig. 9, $p$ increases with the increasing of the CC and reaches 1 when CC = 1. Moreover, large $r$ can also result in a large $p$. When CC=0.94 and $r=0.6$, the $p$ is about 0.85 and the SKD rate is about 10.2 Gb/s. The security of the SKD relies not only on the confidentiality of the synchronized chaos but also on the DNA-key. The former is majorly dependent on the hardware security, for instance the injection and feedback strength, the bandwidth of the MZM, phase bias and time delay between the EOs. According to our results, the utilized chaos synchronization can be very sensitive to the parameter mismatch, especially to the mismatches of bias phase and time delay of the feedback loop. The latter is because that the random DNA coding based on the DNA-key can provide an addition encryption to the SKD. The initial DNA-key is random and can be generated by the Hash function. The eavesdropper cannot regenerate the legitimate key without the DNA-key, though he can crack the synchronized physical entropy. It is noted that even the initial DNA-key is arranged before the SKD, it can update itself based on the SKD. Therefore, a tremendously DNA-key space can be deployed easily. It is worth to note that the randomness of the DNA-key plays a significant role in the SKD, as it matters the anti-crack ability and randomness of the secure.
An ultrafast SKD based on random DNA coding and chaos synchronization in EOs with a common injection is demonstrated numerically. In the scheme, identical EOs are deployed as the nonlinear scramblers to observe the common injected signal and generate synchronized chaos, which can be used as physical entropy of the secure key after photodiode conversion and the self-heterodyne. Dual-threshold sampling is adopted to improve the consistency of the key. In addition, the random DNA coding is introduced to amplify the randomness of the initial binary sequence. Benefit from the random DNA coding and delay DNA-XOR, SKD with a sampling rate of 20 Gb/s can pass the NIST 800-22 tests. Taking the retain ratio of the dual thresholds and the synchronization errors induced by parameter mismatch into account, the final rate of SKD is over 10 Gb/s with a BER below $3.8 \times 10^{-3}$. Moreover, even high-quality synchronization between the responses of OEs can be achieved in a large operation range of injection and feedback factors, the cross-correlation coefficient between the injection and response can be limit to no more than 0.4 by properly adjusting the injection and feedback parameters. The synchronization between the responses is also very sensitive to the mismatch of time delay and phase bias. Therefore, it will be very difficult for the eavesdropper to regenerate the same physical entropy. Furthermore, the random DNA-coding can provide an additional encryption to the secure key, which can greatly enhance the security.

REFERENCES

Chenpeng Xue was born in 1990 in Henan, China. He received the B.S. and the Ph.D. degrees from the University of Electronic Science and Technology of China, Chengdu, China, in 2013 and 2019 respectively. He is currently working with the Advanced Photonics Technology Lab, College of Electronics and Optical Engineering & College of Microelectronics, Nanjing University of Posts and Telecommunications, Nanjing, 210023, China. His dissertation work focuses on the chaos synchronization and photonic microwave generation base on the nonlinear dynamics of semiconductor laser.

Hongdan Wan received the Ph.D. degree from Southeast University, Nanjing, China, in 2013. She is currently a Professor with the Advanced Photonic Technology Lab, School of Optoelectronic Engineering, Nanjing University of Posts and Telecommunications, Nanjing, 210023, China. Her dissertation work focuses on the chaos synchronization and photonic microwave generation base on the nonlinear dynamics of semiconductor laser.

Ping Gu received the Ph.D. degree in physics from Nanjing University, Nanjing, China, in 2016. He is currently a Lecturer with the College of Electronic and Optical Engineering and College of Microelectronics, Nanjing University of Posts and Telecommunications, Nanjing, China. Her research interests include fiber lasers, nonlinear optics, fiber optics, and fiber sensors.

Ning Jiang (M’12) was born in Sichuan, China, in 1984. He received the B.S. degree in communication engineering from the University of Electronic Science and Technology of China, Chengdu, China, in 2005 and the Ph.D. degree in communication and information system from the Southwest Jiaotong University of China, Chengdu, China, in 2012. He is currently an Associate Professor with the School of Information and Communication Engineering, University of Electronic Science and Technology of China. He has authored or co-authored more than 80 research papers. His current research works focus on the all-optical secure communication, and energy-efficient optical access network. He is also a member of Optical Society of America, and a Reviewer of the IEEE Photonics Technology Letters, the Optics Express, the Optics Letters, the Journal of Lightwave Technology, the IEEE Journal of Quantum Electron, the IEEE Photonics Journal, the Applied Optics, Optics Communications, and some other journals.

Yanhua Hong (M’15) Yanhua Hong received the B.Sc. degree in physics from Fujian Normal University, Fuzhou, China, in 1987, the M.S. degree in physics from Beijing Normal University, Beijing, China, in 1990, and the Ph.D. degree in optics from the Institute of Physics, Chinese Academy of Sciences, Beijing, in 1993. She was a Lecturer with Beijing University, Beijing in 1993 and became an associate professor in 1995. Since 1997, she has been with Bangor University, Bangor, U.K., where she became a Permanent Research Staff in 2007, a Lecturer in 2013, and a Senior Lecturer in 2016. She is the author or coauthor of more than 220 journal and conference papers. Her current research interests include microwave photonics, semiconductor laser dynamics, secure key distribution and digital signal processing for high-speed optical communications.

Zuxing Zhang received the Ph.D. degree from Shanghai Jiao Tong University, Shanghai, China. He is currently a Professor with the Advanced Photonic Technology Lab, School of Optoelectronic Engineering, Nanjing University of Posts and Telecommunications, Nanjing, China. His research interests include fiber lasers, nonlinear optics, fiber optics, and optical communications.