photonics

MDPI

Article

Dynamic Secure Key Distribution Based on Dispersion Equalization and Cellular Automata for Optical Transmission

Jiabin Cui, Wei Kong, Zhaoyang Liu and Yuefeng Ji *

State Key Laboratory of Information Photonics and Optical Communications, School of Information and Communication Engineering, Beijing University of Posts and Telecommunications, Beijing 100876, China
* Correspondence: jyf@bupt.edu.cn

Abstract: This paper proposes a dynamic secure key distribution scheme based on dispersion equalization and cellular automata (CAs). The scheme effectively eliminates the key inconsistency problem caused by imperfect channel reciprocity, and dynamic key sequences can be conveniently generated with large key space in long-haul optical transmission. In the process of communication, the legitimate parties obtain the secure core parameter from the frequency domain equalizer algorithm, and a final key sequence is generated through CA iterations on the basis of the core parameter. The randomness and reciprocity characteristics of the channel ensure the security and uniqueness of the core parameter and final key sequence. With 10G Baud 16 quadrature amplitude modulation over 400 km standard single-mode fiber transmission, the proposed scheme is verified with a free key error rate and an unlimited key generation rate. The security robustness of this scheme was theoretically analyzed and verified by sweeping the eavesdropper's tapping position and improving CA operation processing. The proposed key distribution scheme is compatible with the existing transmission system for different signal modulation formats.

Keywords: key distribution; dispersion equalization; cellular automata; key error rate

Citation: Cui, J.; Kong, W.; Liu, Z.; Ji, Y. Dynamic Secure Key Distribution Based on Dispersion Equalization and Cellular Automata for Optical Transmission. *Photonics* **2023**, *10*, 1308. https://doi.org/10.3390/photonics10121308

Received: 18 October 2023
Revised: 11 November 2023
Accepted: 13 November 2023
Published: 27 November 2023

1. Introduction

In recent years, the development of optical fiber communication technology has led to increasingly important work in modern communication networks. Vital and confidential information should be transmitted and shared only by legitimate parties in the optical fiber link [1]. However, optical fiber communication faces many threats, such as interception, eavesdropping, splitting and other physical infrastructure attacks [2], and more attention should be paid to the security issue of optical fiber communication [3–5]. In particular, it is necessary and challenging to share secret keys between legitimate parties and set up a reliable key distribution scheme for private and secure communication.

Conventionally, most secure key distribution schemes are adopted based on public key encryption algorithms like RSA and Diffie Hellman [6–9], relying on computational complexity. However, the security can be guaranteed solely when the computing ability of the eavesdropper is limited, making these encryption technologies fragile when encountering supercomputing technology [10,11]. With the rapid improvement of computing technology, such as quantum computers, the security of these algorithms will face great challenges. On the contrary, key distribution in the physical layer has attracted increased attention, in light of meeting the requirements of large-capacity and high-speed transmission with high reliability and security [12].

The physical layer security technology of key distribution can be mainly divided into two categories: quantum key distribution (QKD) and traditional physical layer secure key distribution. Theoretically, QKD is regarded as absolutely safe since the eavesdropper can be discovered unconditionally due to the non-replicability of the channel once it enters into the quantum channel [13–17]. However, its sensitivity to noise and losses in the optical

fiber link greatly limits the overall transmission distance and system capacity. In addition, the expensive single photon detectors needed in the implementation of the QKD system impede the wider applications of QKD. Alternatively, secure key distribution focusing on the classical optical fiber transmission link has been gradually considered. Recently, several key distribution schemes have been proposed by utilizing the randomness and reciprocity of the physical layer transmission link [18], such as the schemes employing the Mach Zehnder interferometer (MZI) [19], state-of-polarization Stokes parameters (SPs) with information reconciliation (IR) [20], random phase fluctuation of delayed interferometer (DI) tracking [21] and state of polarization (SOP) with IR [22]. However, the key error rate (KER) of these schemes cannot always be zero, and the achievable transmission distance is short and accompanied by a fixed signal format. Their widespread application value is not significant, but the cost of system design and implementation is still high. Therefore, it is of great significance to explore a key distribution scheme that can meet the zero KER index, reduce link length limitations and meet system cost and scalability requirements.

This paper proposes a key distribution scheme based on dispersion equalization and cellular automata (DECA) over 400 km of standard single-mode fiber (SSMF), which was verified via simulations. The proposed DECA scheme can eliminate the key inconsistency problem effectively, and dynamic key sequences can be simply obtained through digital signal processing (DSP) with a larger key space. Since the chromatic dispersion (CD) characteristic is distributed over the whole fiber link between the legitimate communication parties, Alice and Bob, channel reciprocity can ensure that they receive the same key through DSP for the received signal while eavesdroppers cannot. The DSP processing mainly contains two parts: the frequency domain equalizer (FDE) algorithm and cellular automaton (CA) iterations. By using the FDE algorithm, it can be directly operated in the frequency domain of the signal based on the transfer function of dispersion [23,24]. The computational complexity is small, and the compensation effect is significant. A CA can only change its state at fixed and regular time intervals and according to fixed rules, which depend on the values of the cell itself and the values of its neighbors in certain neighboring regions [25,26]. Receivers can acquire the core parameter from the FDE and finally obtain dynamic secure keys in the combination of the core parameter and CA. The simulation results show that this scheme was successfully performed over 400 km of SSMF with free KER and an unlimited key generation rate (KGR). Furthermore, the security analyses of the scheme were conducted via eavesdropping location scanning and CA processing. Then, the randomness of the secure key sequence was verified using the National Institute of Science and Technology (NIST) test. Since the key is obtained by the DSP part, which operates on the standard optical fiber link, this scheme can be adapted to the current transmission system well with various signal modulation formats.

2. Operating Principle

The implementation of this scheme is mainly based on the randomness and reciprocity of the classical optical fiber bidirectional channel. The randomness ensures that the transmission signal, which is shared between Alice and Bob, is closely related to the physical characteristics of the transmission fiber channel, while Eve, the eavesdropper, cannot obtain the same signal by tapping from the channel. Reciprocity ensures the consistency of the received signal between Alice and Bob.

As shown in Figure 1, the received signal from two legitimate parties will experience the same channel effect in theory [27,28]. In other words, channel transfer functions h_{AB}, h_{BA} estimated by Bob and Alice are the same, that is $h_{AB} = h_{BA}$, while h_{AE} and h_{BE}, as estimated by Eve when eavesdropping on the fiber link, are different:

$$h_{AB} = h_{BA}, h_{AB} \neq h_{AE}, h_{BA} \neq h_{BE} \quad (1)$$

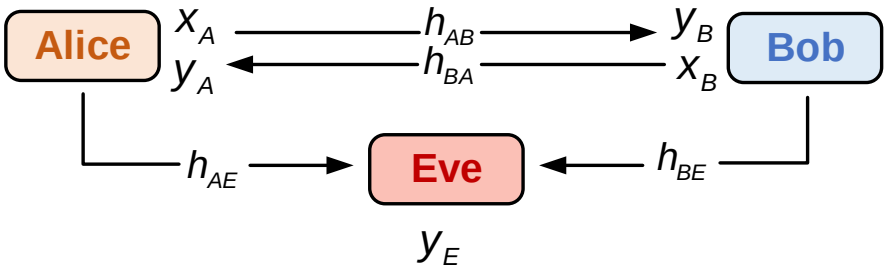


Figure 1. The transmission model of a bidirectional channel.

The signals y_A, y_B and y_E received by Alice, Bob and Eve can be considered as follows:

$$y_A = x_B \times h_{BA} + n_B \tag{2}$$

$$y_B = x_A \times h_{AB} + n_A \tag{3}$$

$$y_E = x_A \times h_{AE} + n_E \tag{4}$$

where x_A, x_B are original transmission signals sent by Alice and Bob, and n_A, n_B and n_E are Gaussian white noise over the experienced fiber channel. However, in wired optical fiber communication,the channel reciprocity may be partially perfect, which is $h_{AB} \neq h_{BA}$, making the signals received by Alice and Bob deviate, resulting in an inconsistency in the key generated from the received signal. In this scheme, the problem caused by channel reciprocity can be effectively solved and verified later via the specific operation processing of the FDE algorithm.

The key distribution scheme based on DECA is shown in Figure 2. It should be noted that two segments of the same optical fiber are set in the local offices of Alice and Bob. It can be reasonably assumed that the local fiber is unknown to Eve, so the CD of the optical fiber is an essential factor in ensuring the security of the key, which makes it impossible for Eve to reconstruct the signal correctly. In this way, Alice and Bob apply the FDE algorithm to the received signal and get the same secure key sequence through CA, while Eve gets the wrong information even if the same DSP processing as the legitimate parties is performed. The specific operation principle will be introduced in the following parts.

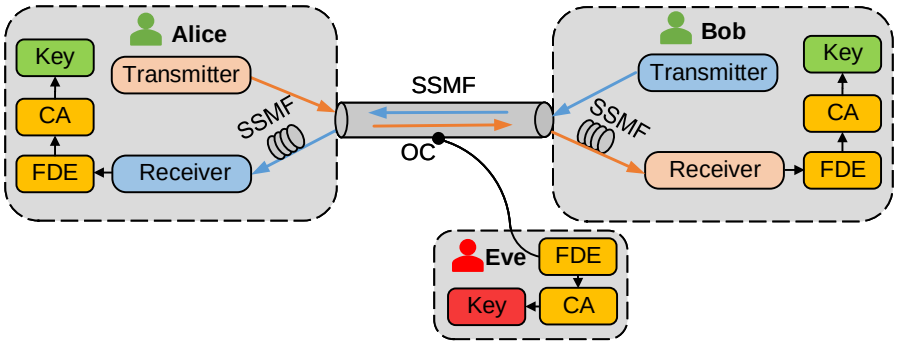


Figure 2. Key distribution scheme based on DECA.

2.1. FDE Algorithm

As the optical signal is transmitted over an optical fiber, the pulse width gradually increases and the peak power of the pulse decreases. When it reaches the receiving side, a significant broadening effect occurs with each pulse becoming wider and overlapping with adjacent pulses. This causes crosstalk between the signals at the receiving end and distortion in the signals, which becomes indistinguishable. This is the dispersion characteristic commonly present in optical fibers, as shown in Figure 3a. Therefore, it is necessary to handle and restore the distorted signals at the receiver. In this paper, the FDE algorithm is

used to compensate for the CD effect of the signal in the electrical domain [23,24]. In the FDE algorithm, the impact of channel dispersion on the transmitted signal can be expressed and calculated using the following formula:

$$G(z,\omega) = \exp\left(-j\frac{D\lambda^2 z}{4\pi c}\omega^2\right) \tag{5}$$

where D is the dispersion coefficient of the optical fiber, which generally used to quantify the optical pulse broadening caused by fiber dispersion, λ is the wavelength of the signal carrier, c is the speed of light, ω is the frequency component and z is the transmission distance. Here, the signal is truncated into several sub-blocks of the same length for dispersion equalization, and then finally combined after operational processing. Therefore, the receiver multiplies the signal by $G^{'}(z,\omega)$, the inverse transfer function of Equation (5), to effectively compensate for the signal spreading caused by CD, which could be expressed as follows:

$$G^{'}(z,\omega) = \frac{1}{G(z,\omega)} = \exp\left(j\frac{D\lambda^2 z}{4\pi c}\omega^2\right) \tag{6}$$

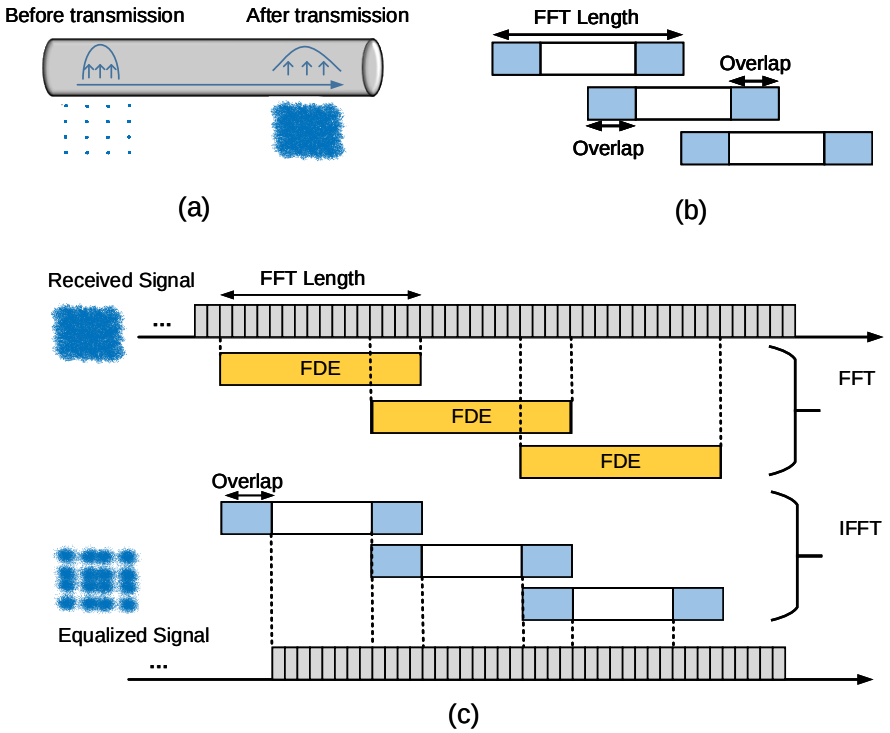


Figure 3. (**a**) Effect of dispersion on signal before and after transmission. (**b**) The first and last intercept length of overlap on each sub-block of FFT length. (**c**) Overlapping FDE algorithm processing, FFT: Fast Fourier Transform, IFFT: Inverse Fast Fourier Transform.

In this scheme, the dispersion coefficient D and the transmission distance z in the dispersion transfer function of Equation (5) are closely related to the specific channel characteristics. Therefore, when the FDE algorithm is adopted, the input parameter of the inverse transfer function in Equation (6), by which the signal is multiplied, represents the whole channel's physical layer characteristics. In order to compensate for and recover the distorted signal better, the overlapping FDE algorithm is introduced here [29,30]. Because the pulse response of the dispersion is symmetrical, there will be a dispersion expansion accumulation of adjacent data blocks at both ends of the sub-block with FFT length after compensating and combining separately, introducing obvious residual dispersion, as shown in Figure 3b. This phenomenon has a great impact on the FDE algorithm, and it is

difficult to highlight the effect of the algorithm on dispersion. Therefore, after compensation processing, keeping a certain proportion of data in each sub-block overlapping with the previous sub-block and discarding the part of overlap length can improve the condition to remove the effect of residual dispersion on the FDE algorithm. Figure 3c depicts the specific procedure of the overlapping FDE algorithm.

Since the input parameter of the FDE algorithm is closely related to the specific optical fiber link and CD is distributed over the entire fiber link, the compensation effect changes with different input parameter values in Equation (6). The variation range and interval of the input parameter can be artificially set to calculate the bit error rate (BER) of the transmitted signal and equalized signal where the lowest BER is considered as the optimal solution, as shown in Figure 4. Due to the experienced different dispersion of the received signals at Alice, Bob and Eve, the optimal solutions of the lowest BER obtained by the same FDE algorithm are definitely different; meanwhile, the input parameter of the FDE algorithm can be regarded as the core parameter secured to distinguish the legitimate parties from the eavesdropper.

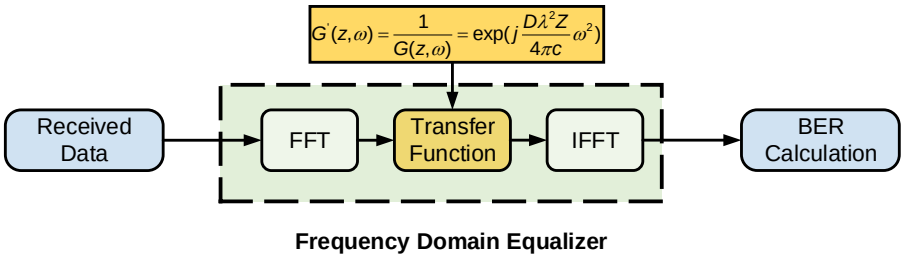


Figure 4. Signal processing of the optimal solution obtained at the receiver side.

This core parameter is obtained by the receiver according to the signal received by itself and by way of only a uniform processing method. Then, the situation with the lowest BER is also determined, that is, the optimal solution of the received signal. The receiver believes that the parameter obtained through processing is unique and correct at this time. Therefore, Eve always believes that the optimal solution obtained by the algorithm is the right parameter information extracted from the currently tapping signal.

Of course, the security of the overall scheme partly comes from the core parameter, so it is expected to expand the key space of this secure parameter further. This parameter is closely related to fiber dispersion coefficient and transmission distance; the variation range is about 10^2~10^3. In addition, a more effective measure is to increase the accuracy of the input parameter variation interval, that is to say, the number of digits after the decimal point. Assuming that the key space is 10^m when the variation interval is an integer, the precision of the variation interval is increased when the number of digits after the decimal point is set as n, and the key space could be significantly improved to 10^{m+n}.

It should be noted that the scheme mainly focuses on the effect of CD on the signal before and after dispersion equalization; only the FDE module is introduced into DSP at the receiver to reflect the trend of BER directly, which is only caused by the input parameter variation of the FDE algorithm, and other DSP modules are not carried out to affect the performance of the FDE algorithm. Therefore, the overall BER remains at a relatively high level, but the trend of BER change is a matter of sole concern, not the specific value.

2.2. CA Iteration

After the FDE module, both legitimate parties of communication will get the same core parameter reflecting the channel dispersion characteristic, which can be processed via cellular automata to obtain the final secure key sequence.

CA is a discrete time model which makes states evolve according to a certain rule, so the definite rule is the kernel of the model [25]. In short, the CA rule is a local state transfer function, that causes global dynamic change by specifying the local function. The inputs of each iteration in CA are the current cell state and neighbor cell states, and the output is the

current cell state of the next time. For example, for one-dimensional cellular automata, the local transformation function can be recorded as follows: $s_i^{t+1} = f(s_{i-r}^t, \ldots, s_i^t, \ldots, s_{i+r}^t)$, where s_i^t is the cell state at position ith and time tth, and r is the neighbor radius. And every cell has one possibility of k states, which means s_i^t is one of k states.

As shown in Figure 5, the effect of FDE is considered the best with the lowest BER and the input parameter at this moment can be seen as the core parameter D_{core} to reflect the channel characteristic. After taking elementary cellular automata (ECA) as an example where $r = 1$ and $k = 2$, and converting Dcore to the rule number D_{rule} of the ECA, $\{b_{000}b_{001}\ldots b_{111}\}$ is the obtained conversion rule of three binary numbers [26], where n is the number of digits after the decimal point of D_{core}:

$$D_{rule} = mod(D_{rule} \times 10^n, 256) \tag{7}$$

$$(b_{000}b_{001}\ldots b_{111})_2 = (D_{rule})_{10} \tag{8}$$

For example, if $D_{rule} = 208 = 2^7 + 2^6 + 2^4$, and the binary number $\{b_{000}b_{001}\ldots b_{111}\} = 11,010,000$, then $f(000) = 1$, $f(001) = 1$, $f(010) = 0$, $f(011) = 1$, $f(100) = 0$, $f(101) = 0$, $f(110) = 0$, $f(111) = 0$. The final secure key sequence K_{final} can be obtained by performing the same periodic CA iterations based on the original key sequence K_{base}, which is pre-shared between Alice and Bob. $K_{j,m}$ is seen as the jth key bit of the mth iteration:

$$(K_{j,m})_2 = b_{(K_{j-1,m-1},K_{j,m-1},K_{j+1,m-1})_2} \tag{9}$$

The length of K_{final} is consistent with the length of K_{base}, and the variation interval of the input parameter can be appropriately increased to prevent D_{core} error caused by channel imperfect reciprocity, thereby effectively ensuring the consistency of the shared key between Alice and Bob. Therefore, the final key sequence is not directly extracted from the received signal performance, and its length is only related to the length of the key base which can achieve unlimited KGR in the proposed scheme. With the improvement of the specific CA design, the key security performance of this scheme will also be improved and dynamic key sequences can be obtained effectively, which will be analyzed in the next part for detailed analysis.

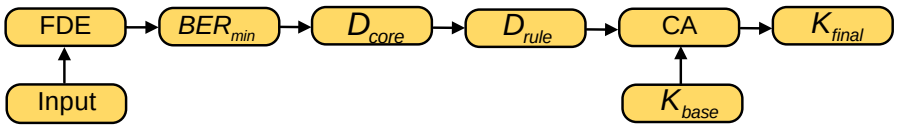


Figure 5. Process of final key sequence generated.

3. Simulations and Discussions

The secure key distribution scheme DECA is verified via simulations which are based on the software of VPItransmissionMaker with the system setup shown in Figure 6. The whole transmission system mainly includes the following parts: Quadrature Amplitude Modulation (QAM) signal generation; fiber link setup, including common fiber link and local fiber link, which is the source of signal experiencing dispersion; a coherent receiver; and DSP modules. At the transmitter, the CW laser (frequency: 193.1 THz, power: 1 mW, linewidth: 100 kHz) is selected as the signal carrier and is modulated using an IQ modulator to generate transmitted QAM signals. To drive the IQ modulator to generate 10G Baud 16QAM signals, respectively, a 40G bps PRBS is employed. Then, the QAM signals generated from Alice and Bob are injected into the common bi-directional transmission link where the dispersion and channel noise are randomly distributed and amplified by EDFA (gain: 20 dB). After the common fiber link, the same local fiber and an OBPF (center frequency: 193.1 THz, bandwidth: 40G Hz) are set at the receiver side. The 90-degree Optical Hybrid and Photo-Diode (PD) are employed to constitute coherent receiver converting

optical signals into electrical signals. After the offline DSP operation and signals resampling, the BER of the input and output signals after the FDE module is depicted and calculated to get the core parameter and generate the final key via CA with $2^{14} = 16,384$ 16QAM signal symbols. Eve, the eavesdropper, is assumed to tap the common fiber link via OC, and tries to acquire the key sequence by processing the received signal with DSP.

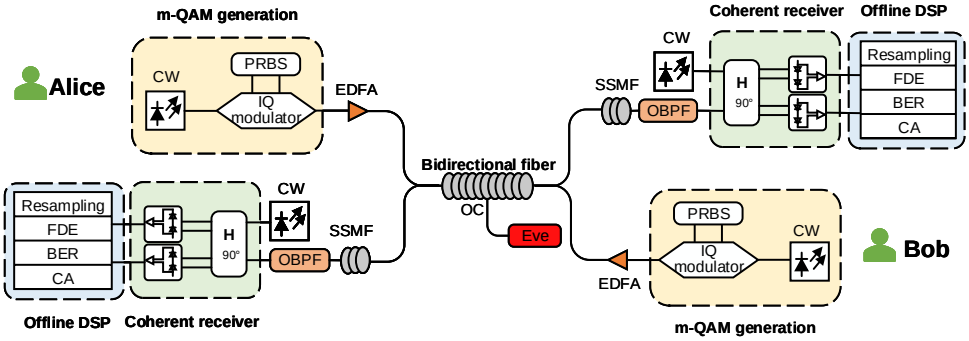


Figure 6. The DECA key distribution scheme system setup based on bidirectional fiber link. CW: continuous wave; PRBS: pseudo random bit sequence; EDFA: Erbium-Doped Fiber Amplifier; OC: optical coupler; OBPF: optical band-pass filter.

It should be noted that, different from other key distribution schemes, the signals sent by Alice and Bob need not be consistent in this scheme, because the relevant information obtained from the received signals is focused on the compensation effect of the FDE algorithm on the signals rather than directly extracting certain signal properties to generate the key. Also, the signals transmitted by Alice and Bob could be transparent. In order to evaluate the security performance of the scheme, Eve cannot eavesdrop in the legitimate office due to the local optical fiber in Alice and Bob, so Eve cannot obtain the same signal as the legitimate receiver. Then, even if Eve has the related information of the common fiber link, due to the uniqueness of the channel and the non-replicable external influence source during the transmission of the optical fiber link, the signals received by Alice and Bob are unpredictable, and Eve cannot obtain the same information. Hence, the core parameters and key sequences obtained by the legitimate parties and the eavesdropper through the specific analyses of the FDE algorithm and CA are compared to later verify the security performance and feasibility of the proposed scheme.

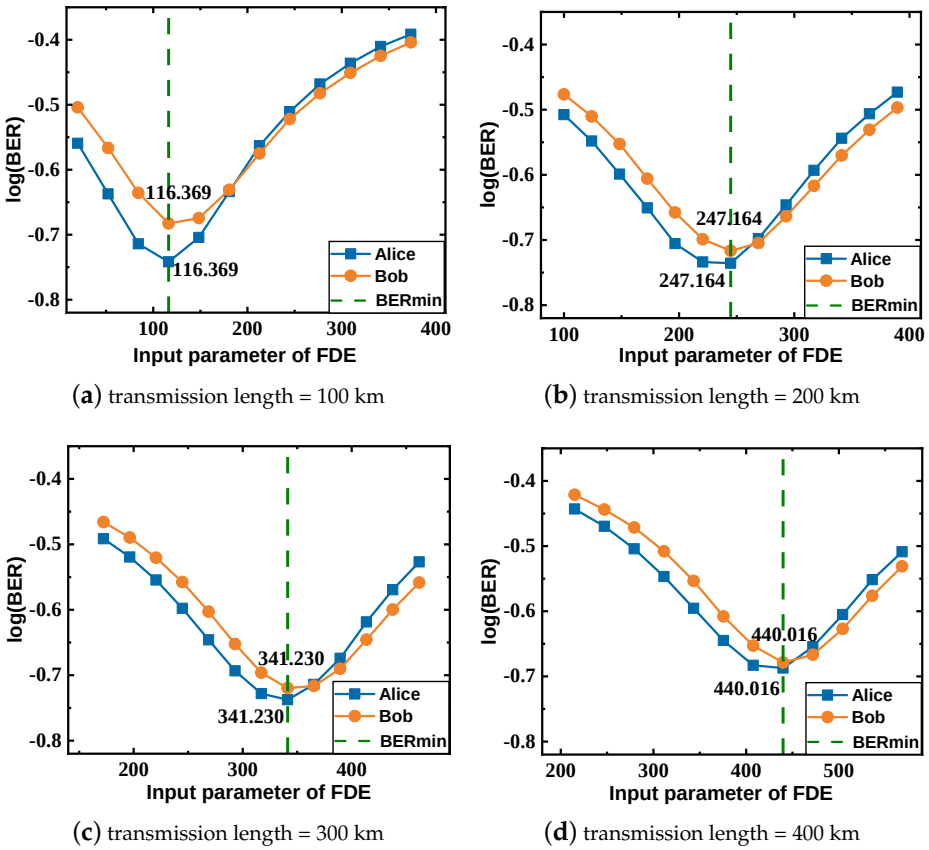
3.1. FDE Algorithm Performance

In the FDE algorithm, during the process of the received signal multiplied with the inverse function $G^{'}(z,\omega)$, the input parameter of function $G^{'}(z,\omega)$ needs to be assigned by oneself, and the BER variation of the receiver can be reflected by changing the input parameter of the FDE algorithm while the compensation effect also changes accordingly, as shown in Figure 7a–d.

By observing and comparing the BER, the optimal solution of the FDE algorithm is the lowest BER, and the input parameter here is seen as the core parameter. The 16QAM signal of 10G Baud is transmitted over the optical fiber link of different transmission lengths, and corresponding BER variation at the receiving side which green line of the lowest BER represents the optimal solution.

It can be found that, for the optical fiber transmission distance ranging from 100 km to 400 km, the legitimate parties, Alice and Bob, could always get the same optimal value D_{core} according to the lowest BER: D_{core} = 116.369 when transmission distance = 100 km, D_{core} = 247.164 when distance = 200 km, D_{core} = 341.230 when distance = 300 km and D_{core} = 440.016 when distance = 400 km. This means that the signals received by Alice and Bob have experienced the same channel upon which random dispersion is distributed on the overall fiber link. Furthermore, their BER variation shows a similar tendency

and has the same lowest point, which ensures consistency and security between the two legitimate parties.



(**a**) transmission length = 100 km (**b**) transmission length = 200 km

(**c**) transmission length = 300 km (**d**) transmission length = 400 km

Figure 7. (**a**–**d**) The BER changing trend with input parameter variation of FDE on different transmission lengths.

3.2. Effective Elimination of Key Inconsistency

Nevertheless, the channel reciprocity is not completely established in the wired fiber-optical transmission link [20,31,32], which means that the signals received by Alice and Bob may not be completely the same. Therefore, in the previous secure key distribution research, the key information is usually extracted directly from the received signal characteristics, like phase fluctuation and SOPs at the receiver side, and the generated key sequence may be inconsistent. In this scheme, the variation interval of the input parameter is set manually, which could be changed. As shown in Figure 8a, it can be found from the simulation results that, when the parameter variation interval is smaller, there will still be an error in the optimal parameter when Alice and Bob both achieve the lowest BER, which will also lead to inconsistency in the key. Along with the increasing of the variation interval to 23.123 represented by the green line limitation, the optimal parameters of Alice and Bob will gradually reach the same values over the 400 km long-distance transmission fiber link.

Figure 8b shows that the KER of Alice–Bob decreases from higher than 30% to zero with the increase of the input parameter variation interval in the FDE algorithm when taking K_{base} = 10011010101100010100111010010 as an example and basically applying ECA. Therefore, compared with the previous schemes, this DECA scheme can effectively and easily eliminate the effect caused by incomplete channel reciprocity, and avoid further additional IR processing for key agreement.

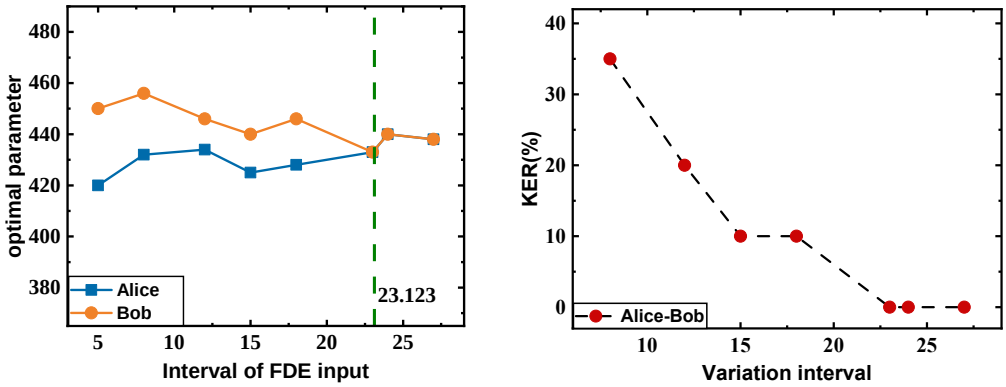


Figure 8. (**a**) The optimal parameter with the variation of FDE input parameter interval where Alice and Bob start to reach the same from green line of interval 23. (**b**) KER between Alice–Bob of different variation intervals.

3.3. Proof of Security under Eavesdropping Attack Situations

In addition, it is more comprehensive to assume that the eavesdropper, Eve, has the same receiver, including specific DSP modules, as the two legitimate parties and has the ability to tap into the standard fiber using the OC before the local receiving side. Considering the multiple possibilities and uncertainty of Eve's attack on the optical fiber transmission link, it could be thought that Eve may try to eavesdrop at different positions of the optical fiber link, aiming to obtain the correct channel characteristic relevant information and obtain a key consistent with Alice and Bob. Therefore, in simulations, it should be taken into consideration that Eve may eavesdrop at each position on the common transmission link, as shown in Figure 9a. The range of positions that Eve can eavesdrop is from A: the leftmost side of the link to B: the rightmost side of the link, and the optimal parameter obtained by Eve at each possible position is compared with the result of Alice and Bob, as shown in Figure 9b.

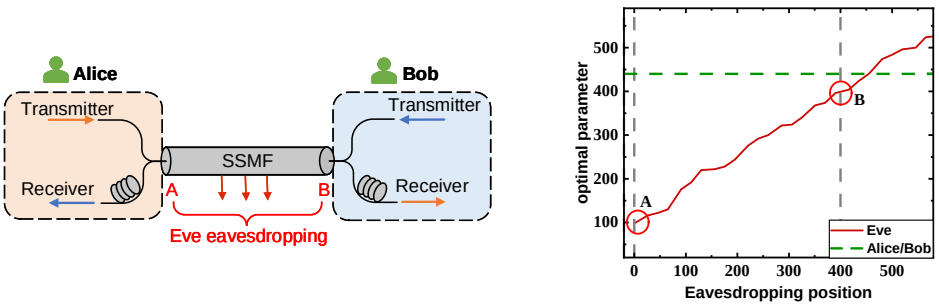


Figure 9. (**a**) Transmission fiber link where eavesdropping position variation ranges from point A to point B. (**b**) Eve's obtained optimal parameter with the eavesdropping position variation compared with Alice–Bob.

It can be seen in Figure 9b that, with the change of eavesdropping position in the common fiber link from point A to point B, which are designated by red circles, the channel characteristic of the received signal is different each time, and the optimal parameter obtained by the FDE algorithm also changes. No matter the position, Eve cannot get the same optimal parameter as the green line limitation of Alice and Bob.

Note that, even if we suppose that Eve can self-connect the fiber by itself, unknown specific local fiber information between Alice and Bob means that Eve wants to try more possibilities to obtain optimal parameters. However, due to each situation where Eve

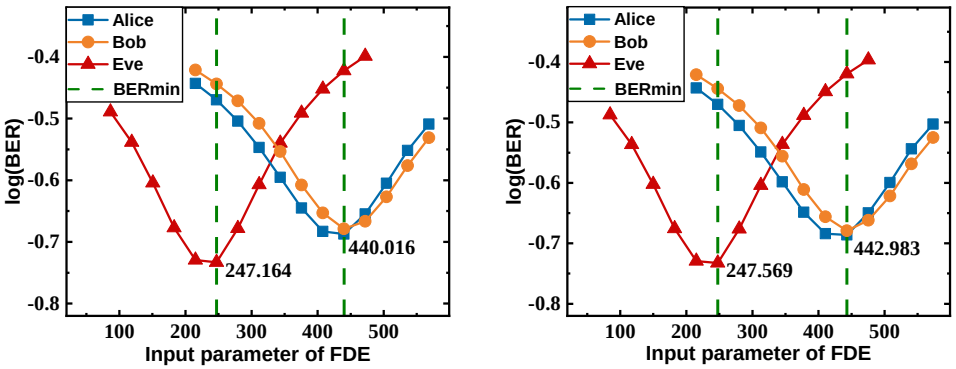
obtains the optimal parameter achieving the best compensation effect at that moment, Eve will always think that the obtained optimal parameter is the only and right parameter. Although Eve self-connects the fiber to a local fiber length that is even longer in Figure 9b, it cannot know which is the same as Alice and Bob and the consistent optimal parameter cannot be obtained. This also proves that the DECA scheme can effectively and strongly resist eavesdropping attacks, and has certain universality and potential for wide application.

3.4. Dynamic Key Generation

For secure key distribution, most schemes aim to establish one optical fiber transmission to generate one key; that is to say, the key obtained in the process of one-time distribution is static and unchangeable. If N key sequences are required, N fiber transmission links need to be established, which greatly increases the cost and complexity of the system construction. In this DECA scheme, dynamic key sequences could be achieved by one fiber transmission process, respectively.

3.4.1. Operation of Input Parameter Variation Interval

On the basis of establishing only one transmission link, the receivers will only obtain one series of signals experiencing the channel. However, the subsequent operation of the received signal is not limited to one time. By changing the variation interval of the input parameter within an appropriate range, multiple core secure parameters are obtained and a dynamic key generation process is formed. Figure 10a,b show the core parameters when the variation intervals are 32.123 and 32.569, respectively. The legitimate parties could always obtain consistent results, and the illegal party could not do so under slightly different variation intervals.



(**a**) variation interval = 32.123 (**b**) variation interval = 32.569

Figure 10. (**a**,**b**) The BER changing trend with different input parameter variation of FDE on Alice, Bob and Eve.

According to former key space analysis for the variable interval, if the precision of the integer part is m and the precision of fractional part is n, the key space of this secure parameter is 10^{m+n}. When the variable interval changes p times to obtain p secure parameters, the key space for the eavesdropper with brute force is $10^{p\times(m+n)}$. It can be seen that this operation can effectively obtain dynamic key sequences through one transmission link, and greatly expand the key space.

3.4.2. Operation of Local Fiber

For both Alice and Bob, they can negotiate specific parameters, such as the length and dispersion coefficient of the local optical fiber in advance, and then operate at the signal receiving side in their respective security zones to ensure uniqueness and consistency between the legitimate parties. According to the scheme design, local optical fibers are set at Alice and Bob's local offices to ensure the security of key information. In the case of a stable common fiber link, the local optical fiber can be changed dynamically and

synchronously between Alice and Bob, so that dynamic key sequences can be generated along with the obtained dynamic optimal parameters. In this way, a dynamic realization of the key distribution and larger key space can be achieved simply and conveniently [33,34]. Meanwhile, with the change of the local optical fiber at both the receiving sides, the signal received by Eve does not experience the local optical fiber, and the parameters obtained by Eve in the process of dynamic change are unchanged and unperceived, causing the change to not be carried out synchronously.

To assess the security performance of this DECA scheme, even supposing that Eve owns the same K_{base} to generate the secure key, it will not be able to get the signals that are experienced through the complete fiber link as well as consistent parameter D_{core}. From Figure 11a, the optimal parameter obtained by Alice and Bob changes, followed by the local fiber variation changing several times. Meanwhile, Eve still obtains the original parameter, which cannot perceive the local fiber changing by tapping into the common fiber. As shown in Figure 11c, the key sequences are definitely different between Alice/Bob and Eve during several instances of local fiber variation. Consequently, Alice and Bob can obtain a changed key sequence each time, while Eve obtains the static key sequence. Hence, the KER of Alice–Bob still remains at zero, but the KER of Alice–Eve always remains at a higher level than 20%, with the same K_{base} shown in Figure 11b.

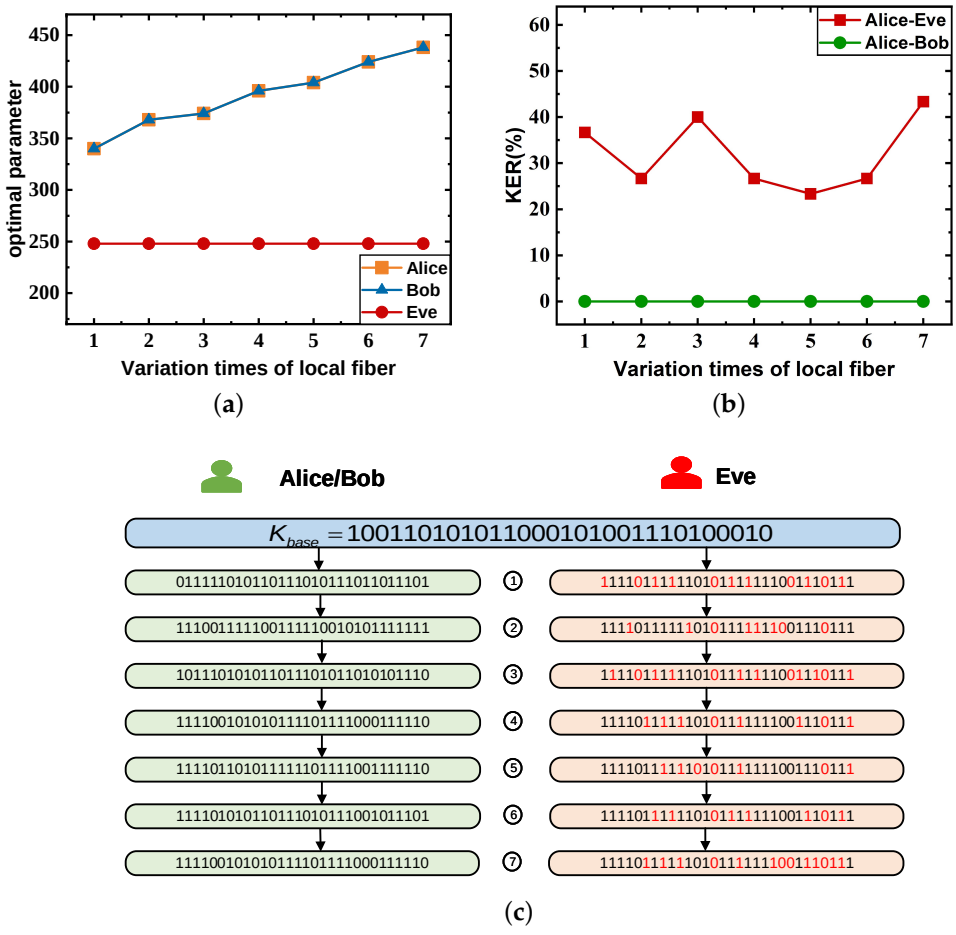


Figure 11. (**a**) Optimal parameter with local fiber variation among Alice, Bob and Eve. (**b**) KER with local fiber variation of Alice–Bob and Alice–Eve. (**c**) Example of dynamic key generation with local fiber variation (The number in red represents an error).

3.4.3. Operation of CA Iteration

Another way to generate a dynamic key is iteration through the CA operation, where each iteration could obtain one key sequence, so N key sequences could be obtained

through N times of iteration simply and conveniently. When the key base and iteration method are certain, Alice and Bob iterate the key base according to the same parameter D_{core}. Even if assumed to have the same K_{base} as Alice and Bob, Eve cannot get the same parameter, and cannot get the final key by iterating the K_{base} with different rules. Therefore, a flexible and efficient dynamic and secure key distribution process is developed, and the key cannot be only fixed in one string.

It can be seen in Figure 12a that, with the variation of iteration time from 1 to 40, taking K_{base} and ECA as an example, the key sequences obtained by Alice and Bob are always identical, and Eve's key sequence has a certain error rate, which remains at a high level. As shown in Figure 12b, the KER of Alice–Bob also remains at zero, while the KER of Alice–Eve is a level higher than 40%. This strongly proves the security and feasibility of key distribution and dynamic key generation.

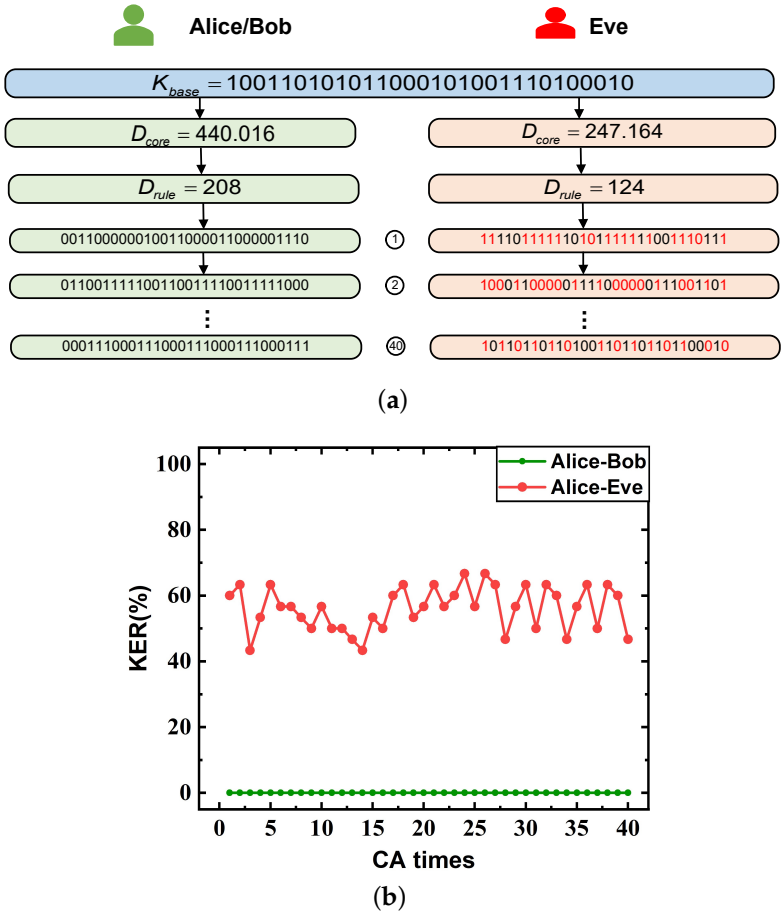


Figure 12. (**a**) Example of dynamic key generation with iteration times from 1 to 40 on the same key base (The number in red represents an error). (**b**) KER with iteration times from 1 to 40 of Alice-Bob and Alice-Eve on the same key base.

3.5. Analysis of Security Enhancement

In the analysis of front parts, CA is always adopted by the most basic automata: ECA with radius $r = 1$, number of cell states $k = 2$ signed by 0 and 1. There are only two possibilities for each cell state and there exists a great risk that, even if the CA rules are inconsistent between Eve and legitimate parties, some of the key bits are maybe the same by chance. Therefore, increasing the number of cell states k can enlarge the key inconsistency between Eve and legitimate parties; the space of cell states and rule number in CA are also expanded significantly, which further greatly expands the key space.

For example, the space of rule number is $2^3 = 8$ when $k = 2$ and $4^3 = 64$ when $k = 4$, such as TGCA [35–37], so the CA rule needs k^3 bits to assign, which represents the

maximum value is 2^{k^3}. When $k = 2$, D_{rule} is used to assign 8 bits, as given in Table 1, and when $k = 4$, the D_{rule} can be applied to ECA in Table 1 and then to assign every 8 bits, as listed in Table 2.

Table 1. CA rule of k = 2 ($D_{core} = 440.016$, $D_{rule} = (208)_{10} = (11010000)_2$).

$(s_{i-1}^t, s_i^t, s_{i+1}^t)$	s_i^{t+1}	$(s_{i-1}^t, s_i^t, s_{i+1}^t)$	s_i^{t+1}
000	1	100	0
001	1	101	0
010	0	110	0
011	1	111	0

Table 2. CA rule with k = 4 ($D_{core} = 440.016$, $D_{rule} = (208)_{10} = (11010000)_2$).

$(s_{i-1}^t, s_i^t, s_{i+1}^t)$	s_i^{t+1}	$(s_{i-1}^t, s_i^t, s_{i+1}^t)$	s_i^{t+1}	$(s_{i-1}^t, s_i^t, s_{i+1}^t)$	s_i^{t+1}	$(s_{i-1}^t, s_i^t, s_{i+1}^t)$	s_i^{t+1}
TTT	A	TTG	C	TTC	G	TTA	T
TGT	C	TGG	A	TGC	T	TGA	G
TCT	A	TCG	C	TCC	G	TCA	T
TAT	C	TAG	A	TAC	T	TAA	G
GTT	T	GTG	G	GTC	C	GTA	A
GGT	G	GGG	T	GGC	A	GGA	C
GCT	G	GCG	T	GCC	A	GCA	C
GAT	T	GAG	G	GAC	C	GAA	A
CTT	C	CTG	A	CTC	T	CTA	G
CGT	A	CGG	C	CGC	G	CGA	T
CCT	T	CCG	G	CCC	C	CCA	A
CAT	G	CAG	T	CAC	A	CAA	C
ATT	T	ATG	G	ATC	C	ATA	A
AGT	G	AGG	T	AGC	A	AGA	C
ACT	C	ACG	A	ACC	T	ACA	G
AAT	A	AAG	C	AAC	G	AAA	T

As shown in Figure 13, the KER between Alice–Bob and Eve of $k = 4$ is generally higher than the situation of $k = 2$. When the number of cell states k is equal to 2, the KER between Alice and Eve is mainly concentrated in the range from 30% to 60%, while ranging from 60% to 90% of k is equivalent to 4, which means that the eavesdropping resistance ability of this scheme is evidently improved by increasing the cell states. The higher the KER, the larger the key error between Eve and the legitimate parties, which strongly enhances the security performance of the final key sequence and improves the confidentiality of the scheme.

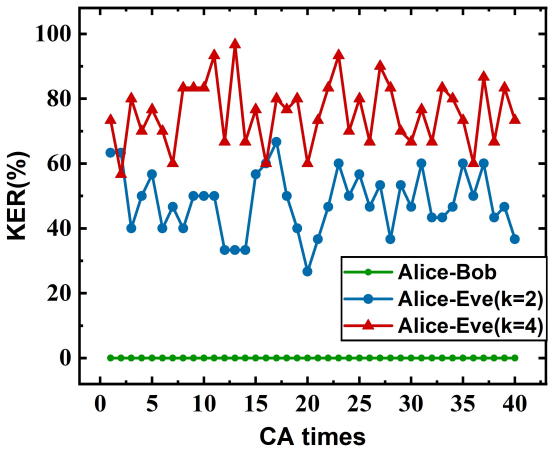


Figure 13. KER with increasing the cell states k among Alice-Bob and Alice-Eve.

3.6. Assessment of Overall Scheme

Compared to other secure key distribution schemes of KER, KGR and overall transmission distance L, it can be seen that the proposed DECA scheme can achieve free KER with longer distances and unlimited KGR, as shown in Figure 14, which means that this scheme has better performance improvement. The specific data values of the comparison scheme here come from relevant references in the literature [19–22].

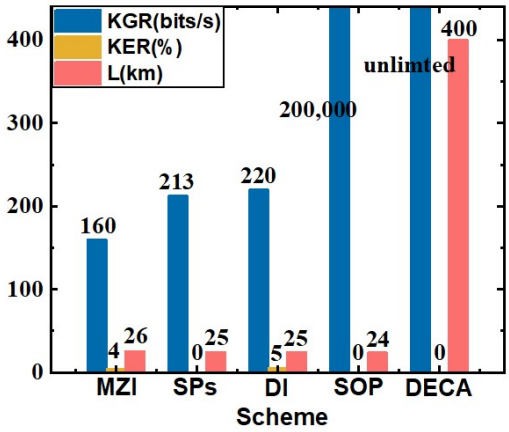
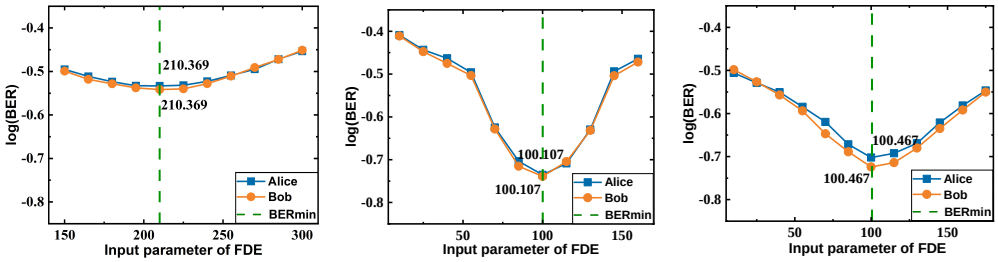


Figure 14. Comparison of different schemes.

Moreover, the 16QAM signal was used as the experimental modulation format in this scheme, which is not necessarily applied in the actual optical fiber application scenario. Therefore, the key distribution scheme based on different and common modulation formats is also simulated and confirmed. As shown in Figure 15a–c, this scheme still holds under low-order and high-order modulation formats of 10 GBaud 4QAM, 32QAM and 64QAM signals. The optimal parameters of the FDE algorithm obtained by Alice and Bob on the receiving sides are different from Eve, which leads to inconsistent key sequences and realizes secure key distribution. Due to the high modulation format, the transmission distance of the optical fiber link is limited to only 100~200 km, which is also a key point that can be considered in further research. Therefore, this key distribution scheme is considered suitable for the transmission system of various modulation formats and has good transmission system adaptability.



(**a**) 4QAM (**b**) 32QAM (**c**) 64QAM

Figure 15. (**a**–**c**) The BER variation with input parameter of FDE for different format signals.

In addition, it is essential to evaluate the randomness analysis of the generated key sequence and the NIST is employed to test this. If all the 15 index test values of the generated key sequence are larger than 0.01, the key can be considered to ensure randomness. In this scheme, the NIST test results of the generated key are listed in Table 3, and all 15 tests are passed, which meets the requirement of the NIST test. Therefore, it can be said that the key sequence distributed by this DECA scheme is random, respectively.

Table 3. Results of the 15 NIST tests.

Index	*p*-Value
Frequency	0.455228
Block frequency	0.042503
Runs	0.746962
Longest Run	0.901933
Rank	0.270256
FFT	0.574617
Non-Overlapping Template	0.999999
Overlapping Template	0.592848
Universal	0.638407
Linear Complexity	0.704754
Serial	0.959372
Approximate Entropy	0.993281
Cumulative sum	0.226876
Random Excursions	0.390989
Random Excursion Variant	0.114968

4. Conclusions

In this paper, a dynamic secure key distribution scheme is proposed and fully analyzed based on DECA. The scheme of 10 GBaud 16QAM over a 400 km transmission is verified via simulations with free KER and unlimited KGR. This scheme can effectively eliminate the influence of channel reciprocity error on the key sequence without post-processing technology. Also, the key space is greatly improved by changing the parameter variation interval slightly, local fiber , and iteration times, in which case dynamic key sequences could be obtained conveniently. Due to the dispersion randomly distributed on the overall fiber, the core parameter is obtained from the FDE algorithm, and put into CA to generate the final key sequence, thus enabling a secure key to be shared between two legitimate parties. Further analysis is carried out to validate the scheme security qualitatively through different wiretapping positions and CA operation settings, showing that the key distribution can be protected in the fiber channel. The simulation results also demonstrate that the generated key meets the randomness requirements of the NIST test, and the scheme can be successfully performed in signal transmission systems with different modulation formats. The proposed scheme is easy to implement without changing the node structure and is well-compatible with current optical transmission systems.

Author Contributions: Conceptualization, J.C. and W.K.; methodology, J.C. and W.K.; software, J.C. and W.K.; validation, J.C. and W.K.; formal analysis, J.C., W.K. and Y.J.; investigation, W.K. and Z.L.; resources, W.K. and Z.L.; data curation, J.C. and Z.L.; writing—original draft preparation, J.C. and W.K.; writing—review and editing, J.C. and Y.J.; visualization, W.K.; supervision, Y.J.; project administration, J.C. and Y.J.; funding acquisition, J.C. and Y.J. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by the National Nature Science Foundation of China (No. 62001046), The Fundamental Research Funds for the Central Universities (2022RC02), and the Fund of the State Key Laboratory of IPOC (BUPT) (No. IPOC2022ZT08), China.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Forutan, V.; Elschner, R.; Schmidt-Langhorst, C.; Schubert, C.; Fischer, R.F. Towards information-theoretic security in optical networks. In Proceedings of the Photonic Networks, 18. ITG-Symposium, Leipzig, Germany, 11–12 May 2017; VDE: Berlin, Germany, 2017; pp. 1–7.
2. Dahan, D.; Mahlab, U. Security threats and protection procedures for optical networks. *IET Optoelectron.* **2017**, *11*, 186–200. [CrossRef]
3. Skorin-Kapov, N.; Furdek, M.; Zsigmond, S.; Wosinska, L. Physical-layer security in evolving optical networks. *IEEE Commun. Mag.* **2016**, *54*, 110–117. [CrossRef]
4. Fok, M.P.; Wang, Z.; Deng, Y.; Prucnal, P.R. Optical layer security in fiber-optic networks. *IEEE Trans. Inf. Forensics Secur.* **2011**, *6*, 725–736. [CrossRef]
5. Shakiba-Herfeh, M.; Chorti, A.; Poor, H.V. Physical Layer Security: Authentication, Integrity, and Confidentiality. In *Physical Layer Security*; Springer: Berlin/Heidelberg, Germany, 2021; pp. 129–150.
6. Bellare, M.; Rogaway, P. Introduction to modern cryptography. *Ucsd Cse* **2005**, *207*, 207.
7. Wang, Y.; Zhang, H.; Wang, H. Quantum polynomial-time fixed-point attack for RSA. *China Commun.* **2018**, *15*, 25–32. [CrossRef]
8. Deshpande, P.; Santhanalakshmi, S.; Lakshmi, P.; Vishwa, A. Experimental study of Diffie-Hellman key exchange algorithm on embedded devices. In Proceedings of the 2017 International Conference on Energy, Communication, Data Analytics and Soft Computing (ICECDS), Chennai, India, 1–2 August 2017; pp. 2042–2047.
9. Yassein, M.B.; Aljawarneh, S.; Qawasmeh, E.; Mardini, W.; Khamayseh, Y. Comprehensive study of symmetric key and asymmetric key encryption algorithms. In Proceedings of the 2017 international conference on engineering and technology (ICET), Antalya, Turkey, 21–23 August 2017; pp. 1–7.
10. Patra, B.; Incandela, R.M.; Van Dijk, J.P.; Homulle, H.A.; Song, L.; Shahmohammadi, M.; Staszewski, R.B.; Vladimirescu, A.; Babaie, M.; Sebastiano, F.; et al. Cryo-CMOS circuits and systems for quantum computing applications. *IEEE J. Solid-State Circuits* **2017**, *53*, 309–321. [CrossRef]
11. Montanaro, A. Quantum algorithms: An overview. *npj Quantum Inf.* **2016**, *2*, 15023. [CrossRef]
12. Wu, Y.; Khisti, A.; Xiao, C.; Caire, G.; Wong, K.K.; Gao, X. A survey of physical layer security techniques for 5G wireless networks and challenges ahead. *IEEE J. Sel. Areas Commun.* **2018**, *36*, 679–695. [CrossRef]
13. Eriksson, T.A.; Trinh, P.V.; Endo, H.; Takeoka, M.; Sasaki, M. Secret key rates for intensity-modulated dual-threshold detection key distribution under individual beam splitting attacks. *Opt. Express* **2018**, *26*, 20409–20419. [CrossRef] [PubMed]
14. Yang, X.; Zhang, J.; Li, Y.; Gao, G.; Zhao, Y.; Zhang, H. Single-carrier QAM/QNSC and PSK/QNSC transmission systems with bit-resolution limited DACs. *Opt. Commun.* **2019**, *445*, 29–35. [CrossRef]
15. Jiao, H.; Pu, T.; Zheng, J.; Xiang, P.; Fang, T. Physical-layer security analysis of a quantum-noise randomized cipher based on the wire-tap channel model. *Opt. Express* **2017**, *25*, 10947–10960. [CrossRef] [PubMed]
16. Zhang, Y.; Chen, Z.; Pirandola, S.; Wang, X.; Zhou, C.; Chu, B.; Zhao, Y.; Xu, B.; Yu, S.; Guo, H. Long-distance continuous-variable quantum key distribution over 202.81 km of fiber. *Phys. Rev. Lett.* **2020**, *125*, 010502. [CrossRef] [PubMed]
17. Fang, X.T.; Zeng, P.; Liu, H.; Zou, M.; Wu, W.; Tang, Y.L.; Sheng, Y.J.; Xiang, Y.; Zhang, W.; Li, H.; et al. Implementation of quantum key distribution surpassing the linear rate-transmittance bound. *Nat. Photonics* **2020**, *14*, 422–425. [CrossRef]
18. Zhang, J.; Marshall, A.; Woods, R.; Duong, T.Q. Efficient key generation by exploiting randomness from channel responses of individual OFDM subcarriers. *IEEE Trans. Commun.* **2016**, *64*, 2578–2588. [CrossRef]
19. Kravtsov, K.; Wang, Z.; Trappe, W.; Prucnal, P.R. Physical layer secret key generation for fiber-optical networks. *Optics Express* **2013**, *21*, 23756–23771. [CrossRef] [PubMed]
20. Zhang, L.; Hajomer, A.A.; Yang, X.; Hu, W. Error-free secure key generation and distribution using dynamic Stokes parameters. *Opt. Express* **2019**, *27*, 29207–29216. [CrossRef] [PubMed]
21. Hajomer, A.A.; Yang, X.; Sultan, A.; Sun, W.; Hu, W. Key Generation and Distribution Using Phase Fluctuation in Classical Fiber Channel. In Proceedings of the 2018 20th International Conference on Transparent Optical Networks (ICTON), Bucharest, Romania, 1–5 July 2018; pp. 1–3.
22. Zhang, L.; Hajomer, A.; Yang, X.; Hu, W. Secure Key Generation and Distribution Using Polarization Dynamics in Fiber. In Proceedings of the 2020 22nd International Conference on Transparent Optical Networks (ICTON), Bari, Italy, 19–23 July 2020; pp. 1–4.
23. Kudo, R.; Kobayashi, T.; Ishihara, K.; Takatori, Y.; Sano, A.; Miyamoto, Y. Coherent optical single carrier transmission using overlap frequency domain equalization for long-haul optical systems. *J. Light. Technol.* **2009**, *27*, 3721–3728. [CrossRef]
24. Kudo, R.; Kobayashi, T.; Ishihara, K.; Takatori, Y.; Sano, A.; Yamada, E.; Masuda, H.; Miyamoto, Y.; Mizoguchi, M. Two-stage overlap frequency domain equalization for long-haul optical systems. In Proceedings of the Optical Fiber Communication Conference, Optical Society of America, San Diego, CA, USA, 22–26 March 2009; p. OMT3.
25. Niyat, A.Y.; Moattar, M.H.; Torshiz, M.N. Color image encryption based on hybrid hyper-chaotic system and cellular automata. *Opt. Lasers Eng.* **2017**, *90*, 225–237. [CrossRef]
26. Naskar, P.K.; Bhattacharyya, S.; Nandy, D.; Chaudhuri, A. A robust image encryption scheme using chaotic tent map and cellular automata. *Nonlinear Dyn.* **2020**, *100*, 2877–2898. [CrossRef]
27. Aldaghri, N.; Mahdavifar, H. Physical layer secret key generation in static environments. *IEEE Trans. Inf. Forensics Secur.* **2020**, *15*, 2692–2705. [CrossRef]

28. Cheng, L.; Li, W.; Ma, D.; Wei, J.; Liu, X. Moving window scheme for extracting secret keys in stationary environments. *IET Commun.* **2016**, *10*, 2206–2214. [CrossRef]
29. Obara, T.; Takeda, K.; Adachi, F. Performance analysis of single-carrier overlap FDE. In Proceedings of the 2010 IEEE International Conference on Communication Systems, Singapore, 17–19 November 2010; pp. 446–450.
30. Tomasin, S. Overlap and save frequency domain DFE for throughput efficient single carrier transmission. In Proceedings of the 2005 IEEE 16th International Symposium on Personal, Indoor and Mobile Radio Communications, Berlin, Germany, 11–14 September 2005; Volume 2, pp. 1199–1203.
31. Huang, C.; Ma, P.Y.; Blow, E.C.; Mittal, P.; Prucnal, P.R. Accelerated secure key distribution based on localized and asymmetric fiber interferometers. *Opt. Express* **2019**, *27*, 32096–32110. [CrossRef] [PubMed]
32. Tu, Z.; Zhang, J.; Li, Y.; Zhao, Y.; Lei, C.; Yang, X.; Sun, Y. Experiment demonstration of physical layer secret key distribution with information reconciliation in digital coherent optical OFDM system. In Proceedings of the 2019 Asia Communications and Photonics Conference (ACP), Chengdu, China, 2–5 November 2019; pp. 1–3.
33. Melki, R.; Noura, H.N.; Mansour, M.M.; Chehab, A. An efficient OFDM-based encryption scheme using a dynamic key approach. *IEEE Internet Things J.* **2018**, *6*, 361–378. [CrossRef]
34. Dang, T.N.; Vo, H.M. Advanced AES algorithm using dynamic key in the Internet of things system. In Proceedings of the 2019 IEEE 4th International Conference on Computer and Communication Systems (ICCCS), Singapore, 23–25 February 2019; pp. 682–686.
35. Sirakoulis, G.C. Hybrid DNA cellular automata for pseudorandom number generation. In Proceedings of the 2012 International Conference on High Performance Computing & Simulation (HPCS), Madrid, Spain, 2–6 July 2012; pp. 238–244.
36. Babaei, A.; Motameni, H.; Enayatifar, R. A new permutation-diffusion-based image encryption technique using cellular automata and DNA sequence. *Optik* **2020**, *203*, 164000. [CrossRef]
37. Wang, Y.; Li, X.W.; Wang, Q.H. Integral Imaging Based Optical Image Encryption Using CA-DNA Algorithm. *IEEE Photonics J.* **2021**, *13*, 1–12. [CrossRef]