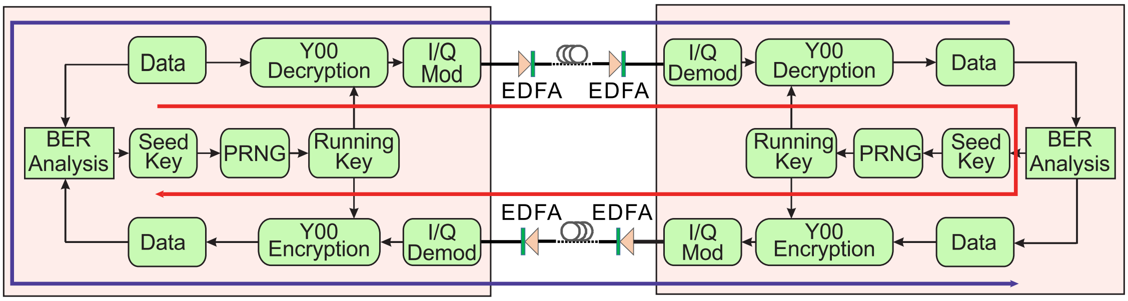
IEEE Photonics Journal
An IEEE Photonics Society Publication

Open Access

Secure Key Distribution System Based on Optical Channel Physical Features

Volume 11, Number 6, December 2019

Xiangqing Wang
Jie Zhang
Yajie Li
Yongli Zhao
Xiaokun Yang



DOI: 10.1109/JPHOT.2019.2953783

Secure Key Distribution System Based on Optical Channel Physical Features

Xiangqing Wang, Jie Zhang, Yajie Li, Yongli Zhao, and Xiaokun Yang

State Key Laboratory of Information Photonics and Optical Communications, Beijing University of Posts and Telecommunications, Beijing 100876, China

DOI:10.1109/JPHOT.2019.2953783

Manuscript received August 26, 2019; revised November 7, 2019; accepted November 11, 2019. Date of publication November 15, 2019; date of current version December 18, 2019. This work was supported in part by the National Natural Science Foundation of China (NSFC) under Grants 61831003 and 61901053 and in part by the joint Foundation of Ministry of Education of China and Department of Equipment Pre-research. Corresponding author: Jie Zhang (e-mail: jie.zhang@bupt.edu.cn).

Abstract: This paper proposes a novel key distribution system based on the measurement of the bit error rate (BER) in a fiber channel. By carrying out the loopback BER measurement at both the transmitting and the receiving end, the BER is quantified and codified to generate consistency keys. Alice and Bob respectively encrypt the signal with the help of the public key base at the transmitting end. At the receiving end the data are decrypted and then the BER is measured. The security of generated keys in the system is enhanced by the use of the encryption base and the randomness of the channel. Additionally, noise sources are added to the channel so that the random noise conceals signals and Eve cannot eavesdrop the useful information in it. Due to the randomness of the channel noise, the generated keys have good randomness. This system at a high key generation rate is compatible with the existing communication device and its measurement is simple. The 10G bit/s-200 km coherent optical communication system is used to measure the BER of the security feature information of the extracted channel. The experimental results show that the key distribution system obtains a consistency rate of 98% with the key generation rate 2 Mbps, both of which have been significantly improved.

Index Terms: Bit error rate (BER), consistency keys, security feature, key generation rate.

1. Introduction

Optical fiber links have been widely used ranging from Ethernet systems to telecommunication backbones as well as other communication areas. They are important infrastructure for high-speed data transmission. Existing fiber links are unable to withstand eavesdropping as well as interception, posing a serious threat to the high-speed interconnect security of critical information infrastructure. In order to resolve the issue, a reliable key distribution system is required to ensure the security of the communication. Therefore, the key distribution technology has a very close impact on network security. Currently, there are two types of self-synchronizing consistency key distribution techniques, including the quantum channel key distribution and the classic channel key distribution.

In the existing physical layer key distribution method, only the Quantum Key Distribution (QKD) protocol can be absolutely secure in theory. Once the eavesdropper accesses the quantum channel, it will be unconditionally discovered by taking advantage of the non-reproducible nature of the single photon [1]. Based on the single-photon coherent one-time protocol, a key distribution is achieved at a rate of 15 bits/s and bulky and expensive single-photon detectors are required [2], [3]. Then the continuous variable quantum key distribution system is proposed [4]–[8], in which the intensity-modulation and simple direct-detection is employed. However, it is only suitable for the short distance transmission and the process of key extraction is more complex. Therefore, it is still desirable to employ a simpler key distribution method in a classic channel at a higher key generation rate.

Researchers have recently proposed generating keys from the randomness of the physical environment, the classic key distribution system. The classical channel key distribution uses the random effect of the classical channel physical layer to generate random keys. The main scheme is a key agreement fiber link based on the polarization mode effect [9]. The polarization mode has good randomness, simple key quantization, a long transmission distance, and low requirements for the environment. The key consistency based on ultra-long fiber lasers makes use of the characteristics of ultra-long fiber lasers to amplify light of a specific wavelength for key negotiation [10], [11]. It has a long key distribution distance, low requirements on equipments and environment, and a fast key distribution rate [12], [13]. However, a more economical key distribution system yet with a high key consistency rate has not been fully explored.

Aiming at the above problems, this paper proposes a key distribution system based on fiber channel physical feature extraction to negotiate consistency keys. The key generation rate in this paper is higher than other papers and the key consistency rate is also better [14], [15]. Since the channel of signal transmission is affected by the interference and the physical effect of various random noises, the channel measurement follows the principle of randomness [16], [17]. It uses the 10 Gbps-200 km experimental transmission platform to add random noises in the process of transmission. Then the loopback measurement is used to send and receive data, and to extract the channel characteristics BER. By analyzing the variation of the BER at both the transmission and the reception end, the consistency key is eventually negotiated. The physical layer channel feature extraction and the key generation together with the key quantization are deeply studied. The experimental results are analyzed from the consistency and randomness of the transceiver.

2. Physical Layer Channel Feature Extraction Principle

In Y-00 [18], binary raw data are multi-level encrypted by the base group. The raw data are immersed in the quantum noise, increasing the complexity of attacker cracking. The security level of Y-00 encryption is higher than the cryptographic algorithm. The legitimate user knows the key and gets the base of each signal. He can process the observed Y-00 signal to recover the original signal information. According to the theoretical research results, the randomized encrypted data (cipher-text) by the quantum noise cannot distinguish the state of the signal base. It is difficult to crack the encrypted cipher-text and the randomization of the quantum noise is an important parameter for evaluating the security, as shown in Fig. 1. It is shown that the binary raw data can be modulated to different amplitude positions for modulation and encryption when the encrypted base M is 8.

At the receiving end, when Alice and Bob use the consistent base, the BER obtained by the loopback measurement is BER_1. Since Eve cannot share the consistent base, the BER of Eve (i.e., BER_2) is higher than BER_1.

Whether the bases of transmitter and receiver are consistent or not, it affects the corresponding BER measurement. Then, the generated keys from BER quantization also change. According to the method of measuring the BER by loopback, the channel feature can be effectively extracted.

The traditional communication system is far away from the noise communication system, and the BER is 0 in far-away zones. The proposed method is close to the noise communication system. The scheme is innovative in that it artificially introduces quantum noise, increases the BER, and achieves superior security by the noise encryption of data. Since the key selection depends on the BER, the consistency lies in the accuracy of the BER.

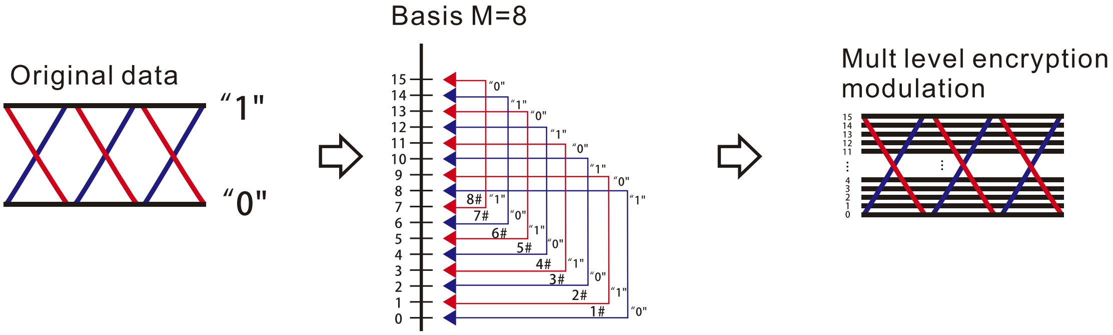
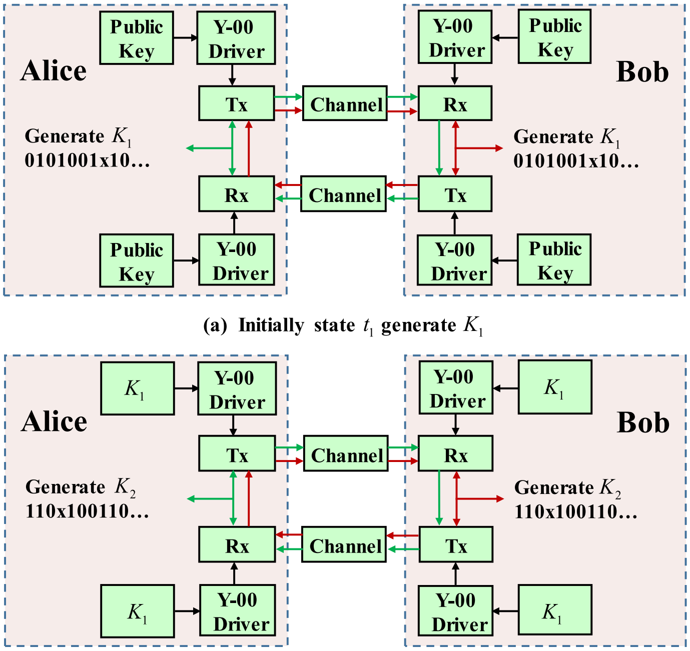


Fig. 1. The principle of encryption Y-00 in different base states.



(a) Initially state t_1 generate K_1

(b) Generate enhanced security K_2 in new state t_2

Fig. 2. The schema of a consistency key negotiated by Alice and Bob from channel physical characteristics BER.

Based on the physical features of the reciprocity and randomness of the channel, the consistency and random keys are generated. Due to the reciprocity of certain devices such as lasers and platforms, the synthesized noise is also reciprocal. The reciprocity of the channel mainly improves the consistency keys while the randomness guarantees random keys. The BER is used as the channel feature of the key generation.

As shown in Fig. 2, the green and the red lines respectively denote the schema of channel physical characteristics BER by loopback measurement from Alice and Bob. As shown in Fig. 2(a), the system mainly employs the physical characteristic BER to generate random and consistency keys. First, Alice uses the public key base to drive Y-00 to encrypt the data which is sent through the transmitter and passes through the channel through Bob, and then Bob sends it back. Alice receives the information through the loopback measurement and decrypts it by Y-00. Then it calculates the BER, and generates the initial key denoted as K_1 by quantizing the password. Similarly, Bob negotiates the consistency K_1 in the way of transmitting the data by loopback measurement and using the reciprocity of the channel and the randomness of the noise to make

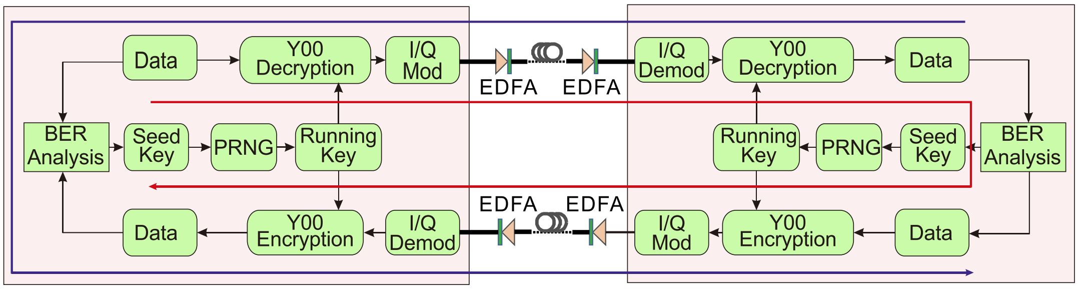


Fig. 3. Design of loopback self-key distribution system for channel feature extraction of optical physical layer.

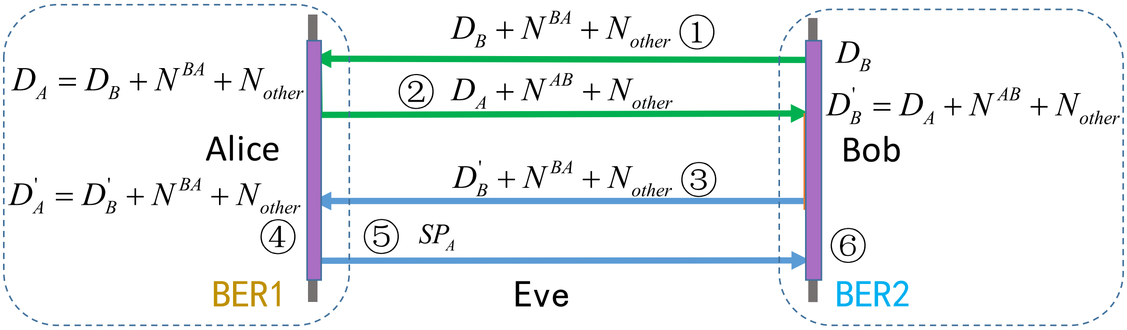

$D_B + N^{BA} + N_{other}$ ①
$D_A = D_B + N^{BA} + N_{other}$
② $D_A + N^{AB} + N_{other}$
D_B
$D_B^{'} = D_A + N^{AB} + N_{other}$
Alice
Bob
$D_B^{'} + N^{BA} + N_{other}$ ③
$D_A^{'} = D_B^{'} + N^{BA} + N_{other}$
④
⑤ SP_A
⑥
BER1
Eve
BER2

Fig. 4. Physics layer key extraction generation principle.

the key generated at the initial state t_1. As shown in Fig. 2(b), K_1 generated by the initial state t_1 encrypts the data, and again uses the randomness and reciprocity negotiation of the channel to generate the enhanced key denoted as K_2. At this time, the initial state t_1 is changed to a new state t_2.

3. Design of Key Distribution System Based on Optical Security Transmission Channel Feature Extraction

3.1 BER Key Extraction Scheme Design

The specific design scheme is as follows. As shown in Fig. 3, the loopback self-key distribution system for physical layer channel feature extraction can be divided into two loopback lines, the first line allows Alice to receive data from Bob. Alice uses the seed key to generate the running key through the pseudo-random number generator, and then encrypts the running key and the data encrypted and transmitted by the optical transmitter. After receiving the data, Bob sends it out according to the same encryption rules. Alice uses the same seed key to generate the running key through the pseudo-random number generator. The running key and the data received by the optical receiver are subjected to error analysis after the de-mapping of the micro-element to obtain the BER. According to the same encryption rule, the second line allows Bob to receive data from Alice basically with the same data processing and equipment as the first line.

In order to increase the BER of the system and quantize the seed key, Alice artificially introduces random noise before sending the signal. Fig. 4 is an exploded view of key distribution based on measurement feature extraction at both ends of the physical layer. In the experiment, these noises have been taken into account. Some noises such as device noise, laser phase noise, and device noise are characterized by slow changes, which can guarantee the BER measured at both ends is slow and reciprocal. Although ASE and Gaussian noise change rapidly and the amplitude is relatively small, the average of the BER after calculating it has little influence on the overall BER.

To calculate the BER, we must know the probability distribution of the synthetic noise at the decision point which mainly comes from the receiver noise and ASE noise. The receiver's own noise includes thermal noise and amplifier noise, which can be considered as a Gaussian probability distribution with a mean of 0. However, the noise $I_n(t)$ distribution of the current introduced by ASE noise is too complicated to be determined accurately since it is amplified, equalized, and finally reaches to the point. For ease of calculation, the synthetic noise at the decision point is approximated as a Gaussian noise distribution so that the BER can be calculated as long as the noise mean and variance are known. In equation (1) when the signals are 0 and 1, the composite noise variance is determined. σ_0 and σ_1 are the synthetic noise variance in the case of signal 0 and 1 respectively. V_0 is the average voltage for the signal. The BER calculation formula can be approximated by (2).

$$Q = \frac{V_0}{\sigma_0 + \sigma_1} \tag{1}$$

$$p_e = \frac{e^{-Q^2/2}}{\sqrt{2\pi}Q} \tag{2}$$

The key distribution rules for physical layer feature extraction are as follows:

Step 1: The data encryption information adopts the Y-00 protocol. First, Bob encrypts the transmission data D_B with the base V-B, then adds noise N^{BA}, and sends the noise-added data $D_B + N^{BA} + N_{other}$ to Alice, N_{other} is the synthetic noise including line noise and receiver noise. The Y-00 encryption protocol is shown in the following formula (3).

$$D_B = \mathrm{mod}[(bit9 \oplus bit0), bit8 \ldots bit0] \tag{3}$$

Step 2: Alice uses Y-00 to solve the encrypted data $D_A = D_B + N^{BA} + N_{other}$ with the same V-B base, and encrypts the newly added data $D_A + N^{AB} + N_{other}$ with Y-00 with the base V-A and sends it to Bob. The Y-00 decryption protocol is shown in equation (4).

$$D'_B = De \bmod [(D_A + N^{AB} - bit8 \ldots bit0) \oplus bit0] \tag{4}$$

Step 3: The data of $D'_B = D_A + N^{AB} + N_{other}$ received by Bob is that Bob solves the encrypted data according to the same Y-00 base V-A. At the same time, the Y-00 based V-B encryption data $D'_B + N^{BA} + N_{other}$ is continuously sent to Alice.

Step 4: Alice decrypts the data $D'_A = D'_B + N^{BA} + N_{other}$ with the base V-B using the Y-00 protocol. At the same time, Alice compares the data sent and received. That is, the data error rate of $D_A = D_B + N^{BA} + N_{other}$ and $D'_A = D'_B + N^{BA} + N_{other}$ is compared, assuming that the total length of the data bits is S, the number of error length bits is S_1, and the bit error rate is $BER_1 = S_1/S$.

Step 5: Assuming that $BER_1 = (0.51, 0.31, 0.32, 0.26, 0.56, 0.35, 0.25, 0.36)_{l=8}$, Alice's BER_1 sequence length is 8, then it is $DS = (1, \times, \times, 0, 1, \times, 0, \times)$ after being quantified and judged. The four bits initial key sequence $KEY_A = (1, 0, 1, 0)$ is generated with the other four discarded. The corresponding position of KEY_A in the sequence of BER_1 is $SP_A = (1, 4, 5, 7)$. The position information SP_A refers to the corresponding position of the initial key sequence KEY_A in the sequence of BER_1. Finally Alice sends the position information to Bob.

Step 6: By the loopback measurement, comparison is made between D'_B Bob receives and D_B Bob sends. The total number of bits is L and the amount of the erroneous information is L_1. The proportion of erroneous information is calculated, that is, the error rate $BER_2 = L_1/L$ obtained by Bob. The position information SP_B is also calculated likewise by Bob. By comparing and matching the position information of Alice SP_A and that of Bob SP_B, a consistency key is finally negotiated.

The BER generated by this system is the bit error rate of loopback transmission, instead of single direction transmission. Both Alice and Bob generate the keys by measuring the BER through the loopback measurement.

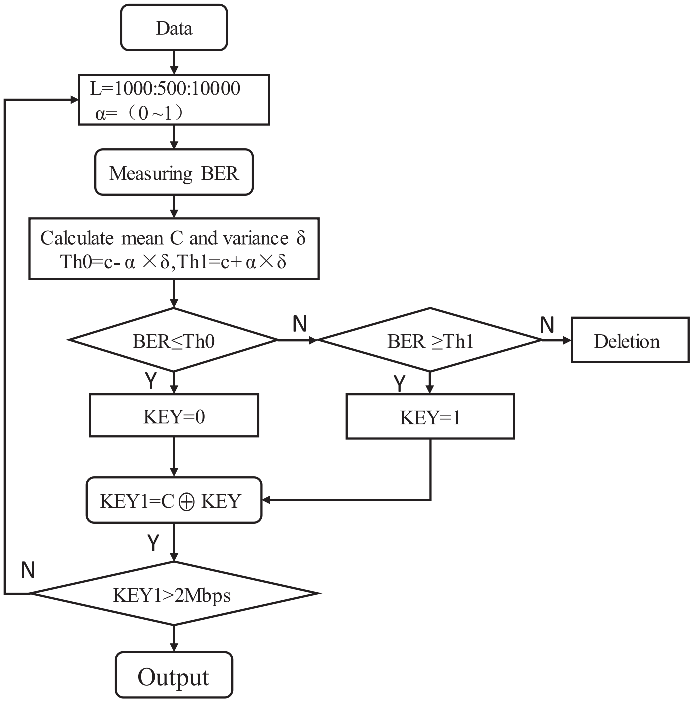


Fig. 5. Adaptive channel feature extraction and generation key flow chart.

3.2 Channel Feature Quantization Technique

Channel feature quantization technology weighs a lot in the decision-making process at the receiving end in that its quality will directly affect the consistency, randomness and independence of the entire key distribution system. Therefore, how to choose the best and determine the reasonable decision threshold is the key to this section. The decision threshold in the scheme is obtained at the average value c, with the point above and below it judged as 1, and 0 respectively.

The specific quantization steps depicted in Fig. 5 are as follows:

Step 1: Calculate the average value c and the variance δ for each set of data of the received data. α is the threshold coefficient, which mainly adjusts key consistency rate and key generation rate.

Step 2: Set the thresholds Th_0 and Th_1, the threshold quantization formula, namely: $Th_0 = c - \alpha \times \delta$, $Th_1 = c + \alpha \times \delta$.

Step 3: When the $BER > Th_1$, quantize it to 1; when the $BER < Th_0$, quantize it to 0.

Among them, the point where the BER is within the range of $(Th_0 - Th_1)$ is discarded, and retained otherwise. This range is set to avoid misjudgment caused by BER disturbances, thus ensuring the consistency of the system.

Fig. 6 shows an experimental diagram for generating a key for channel feature quantization which is realized by firstly blocking the data and then quantizing the generated key according to the calculated threshold values Th_1 and Th_0. The three straight lines on the error rate are thresholds and mean values. According to the BER, a 0, 1 key is generated outside the upper and lower lines, and the data in the two lines is discarded.

4. Analysis and Discussion of Experimental Results

4.1 Experimental Hardware Platform

Fig. 7 depicts the experimental platform for key generation. At the transmitting end, Alice sends a 1550 nm laser through an external laser with an optical power of 12 dBm, and transmits an QPSK

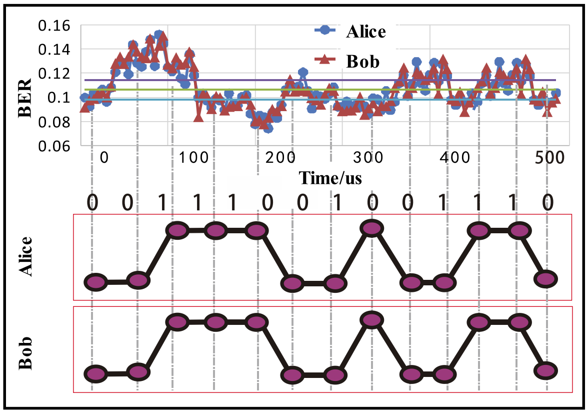


Fig. 6. A key map quantized from channel feature error rate.

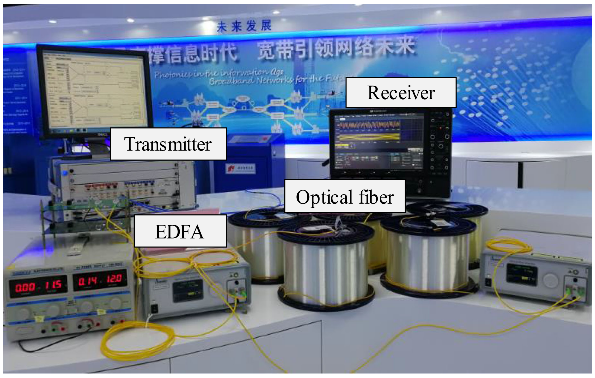


Fig. 7. Experimental platform for key generation.

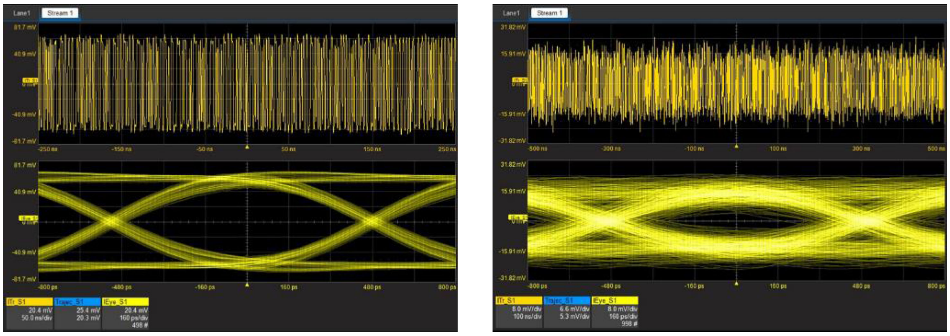
data signal through an intensity modulator. Through the 200 km fiber transmission, the receiving end Bob demodulates the encrypted QPSK signal. Similarly, Bob sends data to Alice, and the two parties share the key base V-A, V-B, demodulate the data, calculate the BER, and coordinate the consistency key by quantization coding. In the case where Eve does not know the base, the error rate of the demodulated signal is too high, and the generated key is inconsistency with the legal side.

4.2 Signal Waveform Diagram and Eye Diagram

As shown in Fig. 8, the QPSK signal is encrypted by the Y-00 protocol. Fig. 8(a) and Fig. 8(b) display the eye diagram of the unencrypted and encrypted QPSK signal after 200 km transmission respectively. The upper and lower edges of the no encrypted eye diagram are clear, but those in the encrypted eye diagram are blurred. While the signal is overwhelmed by noise, the correct signal cannot be resolved.

4.3 Key Generation Performance Analysis

In the experiment, the consistent seed key generated by Alice and Bob becomes the running key through the pseudo-random number generator. And then the running key is detected by the NIST randomness detection standard, as the detection result is shown in Table 1. If the detection result value is less than 0.01, the sequence is determined to be non- random, otherwise random.



(a) No encrypted eye pattern (b) Encrypted eye map signal

Fig. 8. Time Eye pattern comparison before and after transmission signal encryption.

TABLE 1
The Experiment Results of Randomness

No.	Test item	Test index	Test result
1	frequency test	0.735678	Pass
2	block internal frequency test	0.875266	Pass
3	run test	0.225167	Pass
4	longest run test in the test	0.665906	Pass
5	binary matrix rank test	0.197381	Pass
6	discrete Fourier transform test	0.978059	Pass
7	non-overlapping module matching test	0.01117	Pass
8	overlapping module matching test	0.196138	Pass
9	Maurer’s general statistical test	0.948782	Pass
10	linear complexity test	0.292823	Pass
11	sequence test	0.62376	Pass
12	approximate entropy test	0.525363	Pass
13	the accumulation sum test	0.847687	Pass
14	random run test	0.010981	Pass
15	The frequency test of random run state	0.152266	Pass

As shown in Fig. 9(a), the relationship between the length of the selected data and the consistency is direct. The smaller the data block length is, the worse the key consistency is. By quantifying the BER, the consistency of the initial key obtained by Alice and Bob each is as below. The BER interval is gradually increased with the key consistency. When the BER interval is greater than 1.1 μs, the obtained key consistency rate reaches 98%. As the BER measurement interval increases, the error curve is smoother and the fluctuation becomes smaller, so the key consistency quantized by Alice and Bob is improved.

The 0/1 distribution probability of the generated key is shown in Fig. 9(b). As the error measurement interval increases, the 0/1 distribution of the keys generated by Alice and Bob is maintained at about 50%. The better 0/1 distribution means better randomness.

The blue point in Fig. 10(a) is the BER curve measured by Alice, the purple one by Bob and the green one by Eve. It can be seen that the changes in the BER curves of Alice and Bob are basically the same, while the error rate of Eve is obviously high, also accompanied with significantly different trend of change. Therefore, Eve quantifies the error rate by the same method and the key obtained by Alice and Bob. By quantizing the BER, Alice and Bob get a consistency key, as shown

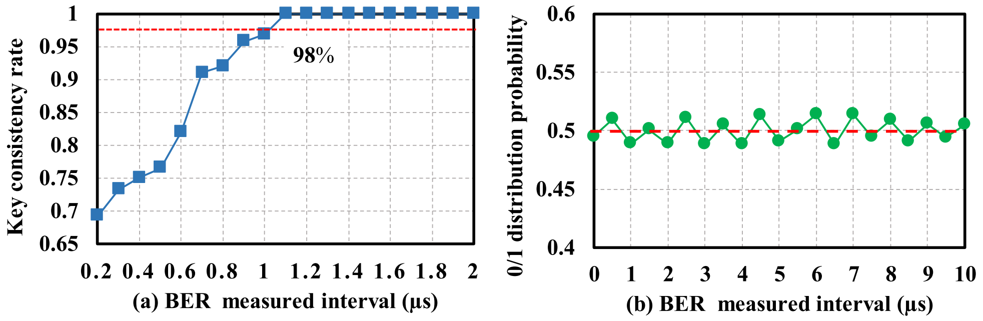


Fig. 9. The relationship between BER measured interval and key consistency rate as well as the 0/1 distribution probability.

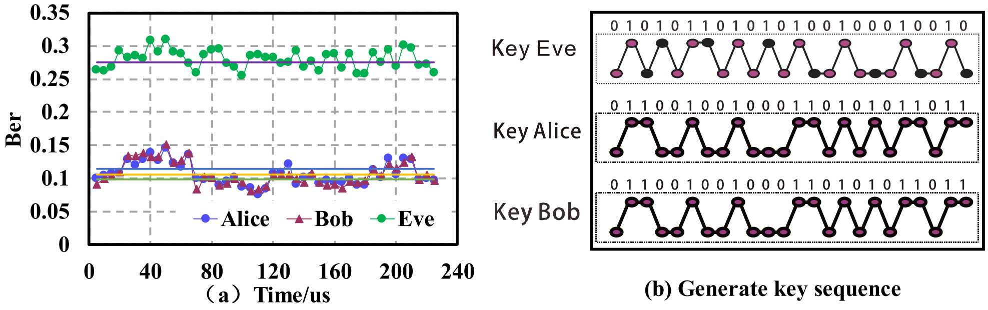


Fig. 10. (a) Key independent experiment analysis result. (b) A security key sequence comparison diagram generated by Alice, Bob and Eve.

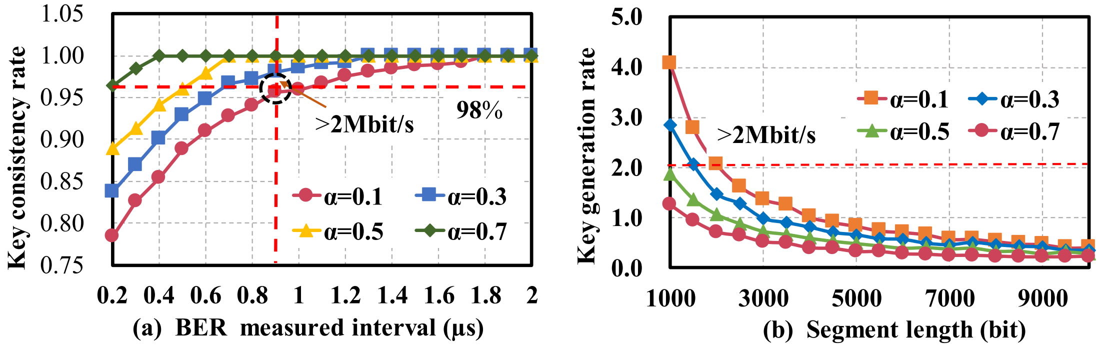


Fig. 11. (a) Relationship between key consistency rate and error measurement interval. (b) Relationship between key generation rate and segment length.

in Fig. 10(b). The key A is the seed key generated by Alice, and the Key B obtained by Bob. A total of 24 bits are generated, and the key code rate is about 2 Mbps. Alice and Bob have a key error rate of zero.

By quantizing the BER, Alice and Bob get a consistency key, but Eve gets a significantly different one, reflecting the irrelevance of key generation. As shown in Fig. 10(a), for the Key Eve, the black solid circle is an inconsistency key and the key error rate is 0.33. Since Eve measures the BER through different devices and lines that are different from those of Alice and Bob, the BER of Alice and Eve will not be exactly the same. The BER is a variable that can be used to negotiate the key, so the generated key is also not the same.

Fig. 11(a) shows the relationship between the BER measurement interval and the key consistency rate in the case of different quantized coefficients α. The BER measurement interval

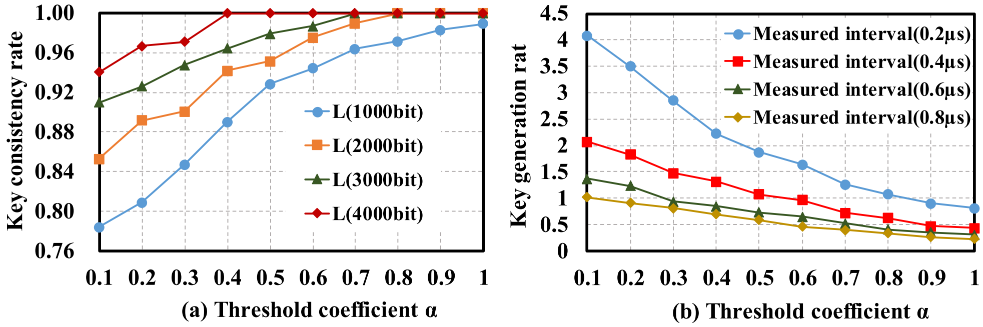


Fig. 12. (a) A diagram of threshold decision coefficient and key consistency rate. (b) A diagram of threshold decision threshold coefficient and key generation rate.

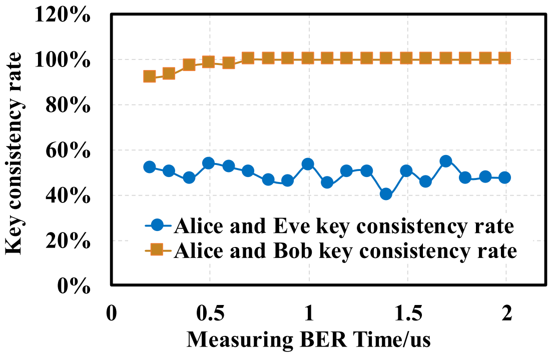


Fig. 13. Alice, Bob and Eve key consistency rate comparison.

increases with the key consistency. When the BER measurement interval is longer than 0.8 μs, the obtained key consistency rate reaches 98%, and key generation rate reaches 2 Mbit/s. The key generation rate denotes the rate of the initial key generated in the experiment. The key distribution rate which is the actual key of operation in the system is smaller than the initial key. The initial key needs to be converted into a distribution key and processed through data. Thus the key generation rate in this paper is higher than other papers and the key consistency rate is also better. As the error rate measurement interval increases, the error curve is smoother and the error fluctuations become smaller, so the key consistency quantized by Alice and Bob is improved. In the case of different quantized coefficients α, the key consistency rate and the BER measurement interval are analyzed. At the same measurement time, as α increases, the key consistency rate increases, but the key generation rate decreases.

Fig. 11(b) depicts the effect of data segmentation length and key quantization coefficient on key generation rate. The data segmentation interval increases with the key generation rate reduced, and in the case of equal segmentation intervals the key generation rate decreases with the increase of the quantization coefficient. When α is between 0.1 and 0.3, the key rate is greater than 2 Mbit/s, and the comprehensive analysis selects α to 0.3, which improves the system performance.

It is shown in Fig. 12(a) the relationship between the threshold coefficient α and the key consistency rate. In the case where the quantized coefficient is constant and the data block length L is 1000 bit–4000 bit, the consistency rate increases with the block length. When the block length L is 3000 bits and the threshold coefficient α is greater than 0.5, the key consistency rate is over 98%. Fig. 12(b) shows the relationship between the threshold coefficient α and the key generation. When the measurement interval length is 0.2 us, 0.4 us, 0.6 us, and 0.8 us and the threshold coefficient is constant, the key generation rate is reduced as the measurement interval increases. When the measurement interval is less than 0.2 us, the key generation rate can reach 4 Mb/s or more.

As shown in Fig. 13, the key consistency rate of Alice and Bob gradually increases with the error measurement interval, which is close to 100%. As the error measurement interval increases, the key consistency rate of Alice and Eve remains near to 50%. The experimental results show that the security feature extraction method and key consistency negotiation scheme adopted in this paper can meet the consistency and security requirements. Repeaters that do not affect the security and randomness of the system will make little difference. And the key distribution distance will increase.

5. Conclusion

The proposed key distribution system adopts multi-level encryption and noise extraction transmission technology to realize line transmission security. It significantly improves the capability in information protection of the physical layer of the optical communication system. The experimental platform of this paper focuses on building a 200 km long-span physical layer security key distribution system. The research has achieved a key generation rate of 2 Mbps with 98% key consistency rate. The key distribution technology adopted in this paper is based on the physical feature extraction. The optical noise inherent in the optical communication process is utilized to directly encrypt the transmission data without affecting the transmission performance of the system. The key distribution system realized by the BER in both the transmitter and the receiver is compatible with existing communication systems. It can encrypt the data and carry out a high-speed, long-distance secure transmission.

References

[1] R. J. Hughes, G. L. Morgan, and C. G. Peterson, “Quantum key distribution over a 48 km optical fibre network,” *J. Mod. Optic.*, vol. 47, no. 2/3, pp. 533–857, 2000.

[2] C. Marand and P. D. Townsend, “Quantum key distribution over distances as long as 30 km,” *Opt. Lett.*, vol. 20, no. 16, pp. 1695–1697, 1995.

[3] A. Tanaka *et al.*, “Ultra-fast quantum key distribution over a 97 km installed telecom fiber with wavelength division multiplexing clock synchronization,” *Opt. Exp.*, vol. 16, no. 15, pp. 11354–11360, 2008.

[4] D. Stucki *et al.*, “High rate, long-distance quantum key distribution over 250 km of ultra low loss fibres,” *New J. Phys.*, vol. 11, no. 7, 2009, Art. no. 075003.

[5] M. Sasaki *et al.*, “Field test of quantum key distribution in the Tokyo QKD Network,” *Opt. Exp.*, vol. 19, no. 11, pp. 10387–10409, 2011.

[6] H. K. Lo, M. Curty, and K. Tamaki, “Secure quantum key distribution,” *Nature Photon.*, vol. 8, no. 8, pp. 595–604, 2014.

[7] P. Jouguet, S. Kunz-Jacques, A. Leverrier, P. Grangier, and E. Diamanti, “Experimental demonstration of long-distance continuous-variable quantum key distribution,” *Nature Photon.*, vol. 7, no. 5, pp. 378–381, 2013.

[8] B. Korzh *et al.*, “Provably secure and practical quantum key distribution over 307 km of optical fibre,” *Nature Photon.*, vol. 9, no. 3, pp. 163–168, 2015.

[9] I. U. Zaman, A. B. Lopez, M. A. Al Faruque, and O. Boyraz, “Polarization mode dispersion-based physical layer key generation for optical fiber link security,” in *Proc. Opt. Sensors, Opt. Soc. Amer.*, 2017, Paper JTu4A-20.

[10] A. Zadok, J. Scheuer, J. Sendowski, and A. Yariv, “Secure key generation using an ultra-long fiber laser: Transient analysis and experiment,” *Opt. Exp.*, vol. 16, no. 21, pp. 16680–16690, 2008.

[11] O. Kotlicki and J. Scheuer, “Secure key distribution over a 200 km long link employing a novel ultra-long fiber lasers (UFL) scheme,” in *Proc. Conf. Lasers Electro Opt./Quantum Electron. Laser Sci. Photon. Appl. Syst. Technol., Tech. Dig. (CD), Opt. Soc. America*, 2010, Paper ATuA4.

[12] A. El-Taher, O. Kotlicki, P. Harper, S. Turitsyn, and J. Scheuer, “Secure key distribution over a 500 km long link using a Raman ultra-long fiber laser,” *Laser Photon. Rev.*, vol. 8, no. 3, pp. 436–442, 2014.

[13] J. Scheuer and A. Yariv, “Giant fiber lasers: A new paradigm for secure key distribution,” *Phys. Rev. Lett.*, vol. 97, no. 14, 2006, Art. no. 140502.

[14] A. A. Hajomer, X. Yang, A. Sultan, and W. Hu, “Key distribution based on phase fluctuation between polarization modes in optical channel,” *IEEE Photon. Technol. Lett.*, vol. 30, no. 8, pp. 704–707, Apr. 2018.

[15] I. U. Zaman, A. B. Lopez, M. A. A. Faruque, and O. Boyraz, “Physical layer cryptographic key generation by exploiting PMD of an optical fiber link,” *J. Lightw. Technol.*, vol. 36, no. 24, pp. 5903–5911, Dec. 2018.

[16] M. Nakazawa, M. Yoshida, T. Hirooka, and K. Kasai, “QAM quantum stream cipher using digital coherent optical transmission,” *Opt. Exp.*, vol. 22, no. 4, pp. 4098–4107, 2014.

[17] M. Nakazawa *et al.*, “QAM quantum noise stream cipher transmission over 100 km with continuous variable quantum key distribution,” *IEEE J. Quantum Electron.*, vol. 53, no. 4, Aug. 2017, Art. no. 8000316.

[18] T. Nishioka, T. Hasegawa, H. Ishizuka, K. Imafuku, and H. Imai, “How much security does Y-00 protocol provide us?” *Phys. Lett., A.*, vol. 327, no. 1, pp. 28–32, 2004.