photonics

MDPI

Communication

Combined Optical Fiber Transmission System Based on QNSC and BER-LM

Xiaokun Yang [1], Xiangqing Wang [2,*], Dongfei Wang [1,3], Lan Zhang [1], Zufang Yang [1], Han Zhu [1] and Baohong Wu [1]

[1] School of Artificial Intelligence, Wuhan Technology and Business University, Wuhan 430065, China
[2] School of Physics and Electronic Engineering, Fuyang Normal University, Fuyang 236037, China
[3] School of Information Engineering, Beijing Institute of Graphic Communication, Beijing 102600, China
* Correspondence: wxqing@fynu.edu.cn; Tel.: +86-147-9020-1963

Abstract: A quantum noise stream cipher (QNSC) is a physical layer encryption technology based on quantum noise. Bit error rate loopback measurement (BER-LM) is a method to measure the BER of a loopback channel and extract channel characteristics. Then, channel characteristics can be extracted, and consensus keys can be obtained through negotiation. In previous studies, encryption and key distribution were implemented in independent channels. In this paper, we propose a scheme that combines these two technologies in a single fiber channel to achieve encrypted transmission and key distribution. We verified a 20 Gbps QPSK coherent optical transmission system with a PSK/QNSC scheme. The results show that by reasonably setting the negotiation bit position, the consensus key could be obtained through negotiation, and the requirements of transmission performance could be met. When the negotiation bit position was set to seven, the Q-factor of the system was nine, which met the error-free condition of the 7% forward error correction (FEC) limit.

Keywords: physical layer; key distribution; quantum noise stream cipher; optical fiber communication

check for updates

Citation: Yang, X.; Wang, X.; Wang, D.; Zhang, L.; Yang, Z.; Zhu, H.; Wu, B. Combined Optical Fiber Transmission System Based on QNSC and BER-LM. *Photonics* **2023**, *10*, 154. https://doi.org/10.3390/photonics10020154

Received: 1 November 2022
Revised: 13 January 2023
Accepted: 16 January 2023
Published: 2 February 2023

Copyright: © 2023 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

In order to realize the security of an optical fiber physical layer, optical fiber physical layer encryption technology and physical layer key distribution technology are the current research focus. QNSC is a representative optical fiber physical layer encryption technology [1–4]. It masks the original signal through high-order QAM or PSK modulation to improve transmission security [5–7]. In the previous paper, by measuring the bit error rate (BER) of the optical fiber loopback channel, the communication parties could negotiate to obtain a consistent key through quantization coding [8,9]. The influence of polarization mode dispersion (PMD) on legitimate communication parties is similar, which ensures that both parties can negotiate to obtain a consistent key [10]. In 2008, the California Institute of Technology proposed a key distribution scheme using ultralong fiber lasers [11–15]. The quantum inseparability and immeasurability can also be used for key distribution [16–18].

In general, a physical layer encryption scheme and a key distribution scheme are implemented in mutually independent channels. For example, the classical optical fiber encryption transmission channel cannot be compatible with the quantum key distribution (QKD) channel. The key distribution system based on ultralong fiber lasers cannot transmit encrypted signals. Because the classical encryption channel and key distribution channel are incompatible, the limited fiber channel resources cannot be fully utilized, resulting in a waste of spectrum resources, increasing system complexity and equipment costs.

In this paper, based on the combination of QNSC and BER-LM, an integrated method of encryption transmission and key distribution in a single optical fiber channel is proposed. The feasibility of this method was verified by simulation. The simulation demonstrated that in the coherent transmission system of a single wavelength fiber channel, encrypted data transmission and key distribution could be realized simultaneously, and the data transmission rate was 20 Gbps. We compared the impacts of different key agreement bits

on the performance of encrypted transmission. When the negotiation bit was set to seven, the Q factor of the encrypted transmission signal was nine, which met the transmission performance requirements.

2. Integrated Architecture of QNSC and BER-LM

2.1. Principle of PSK/QNSC

The principle of QNSC was first proposed in an article published in 2004, which indicated that information-theoretic security against a known-plaintext attack is possible with QNSC [19]. Figure 1 illustrates the process of transforming a 2PSK signal into an encrypted 8PSK signal through PSK/QNSC. The 2PSK signal has only two angles with a difference of 180 degrees, corresponding to 0 and 1, respectively, which can represent 1-bit data. A 2-bit key (k1 and k2) can have four forms (00, 01, 10, and 11) and can represent four directions. With PSK/QNSC, a 2PSK signal is rotated to four directions to obtain an encrypted 8PSK signal. For example, by using the 1-bit data D = 0 and the 2-bit key K = (k0, k1) = (0, 1), the 2-bit encrypted data E = (k0, k1 $\oplus$ b) = (0, 1) can be generated. Then, the 2-bit encrypted data can be mapped to the 8PSK constellation. By increasing the bit number of the key, you can further obtain encrypted data of 16PSK, 64PSK, . . . , 2nPSK. With the increase in the bit number of encrypted data, constellation points become more and more dense, and adjacent constellation points are more easily masked by optical noise generated by amplifiers and lasers. This can prevent Eve from identifying accurate signals without knowing the key. The legal receiver can use the key to recover the original 2PSK signal and obtain accurate original data.

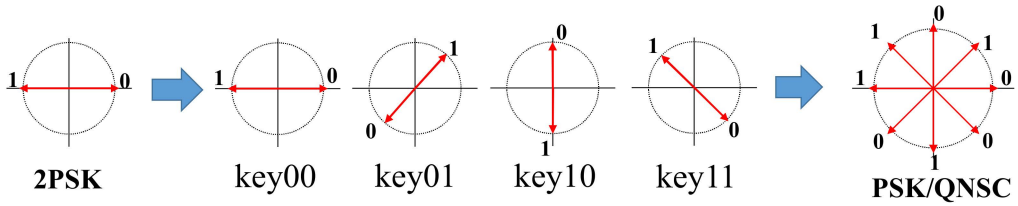

Figure 1. A 2PSK signal encryption procedure with a PSK/QNSC scheme.

2.2. Key Generation Based on BER-LM

$$K(n) = \begin{Bmatrix} 1, & BER \geq Thr_{upper} \\ 0, & BER < Thr_{lower} \\ x, & others \end{Bmatrix} \quad (1)$$

The key distribution scheme was proposed in an article that obtained channel characteristics by measuring the SNR of the optical fiber channel and generating the consistent key by quantization coding [9]. As shown in Figure 2, Alice and Bob measure the BER of the loopback fiber channel from both ends of the fiber channel. At the same time, the BER of the loopback fiber channel remains unchanged, so Alice and Bob can obtain the same BER curve. Take the BER sampling points in a period of time, calculate the average (δ) of the BER sampling value, and calculate the variance (σ) of the BER sampling value. Quantify the BER sampling values according to formula (1), where $Thr_{upper} = \sigma + \delta$ and $Thr_{lower} = \sigma - \delta$. When BER is higher than Thr_{upper}, the quantization value is 1; when BER is lower than Thr_{lower}, the quantization value is 0. When BER is between Thr_{upper} and Thr_{lower}, discard the BER sample value, which can improve the consistency of the quantization results.

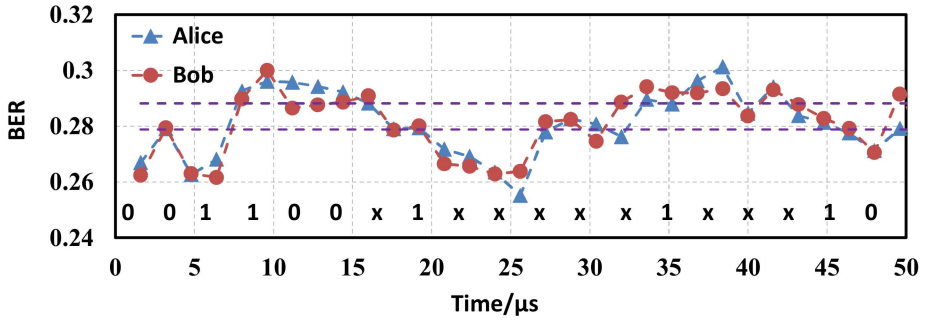

Figure 2. BER of loopback fiber channel measured by Alice and Bob.

2.3. Transmission and Negotiation Integrated Transformation

Figure 3a shows the process of encrypted transmission over the optical fiber channel. The key distribution channel transmits the key to the legitimate sender and receiver. The sender encrypts the original data with the key, and the receiver can recover the original data with the key. Figure 3b shows the principle of transmission and negotiation integrated transformation (TNIT). As shown in Formula (2), the negotiation data (d) can be XOR with any bit except the highest bit (k9). The transmitted data (d) can only be XOR with the highest bit (k9) of the key to obtain the encrypted data (E).

$$E = f(d,\ b,\ key) = (k0,\ k1,\ \ldots,\ k6 \oplus b,\ k7,\ k8,\ k9 \oplus d) \tag{2}$$

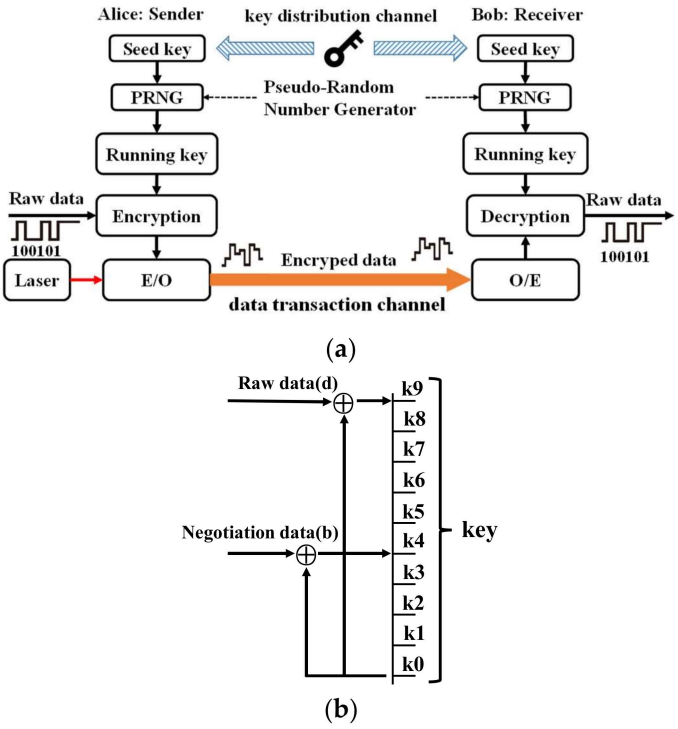

Figure 3. (**a**) Encryption transmission principle of optical fiber communication. (**b**) Principle of transmission and negotiation integrated transformation.

3. Integrated System of QNSC and BER-LM

Figure 4 shows the system schematic diagram of QNSC and BER-LM. The raw data, negotiation data, and operation key are generated by Alice. After bit mapping of TNIT, encrypted data can be obtained. The encrypted data are sent to Bob through the optical transmitter, and Bob receives the signal through the optical receiver. Bob uses the running key to obtain the received data and negotiation data through bit demapping. Alice and Bob use the loopback negotiation data to calculate the BER. The BER samples are quantized and

encoded to obtain the seed key. Then, the seed key generates the running key using the random number generator.

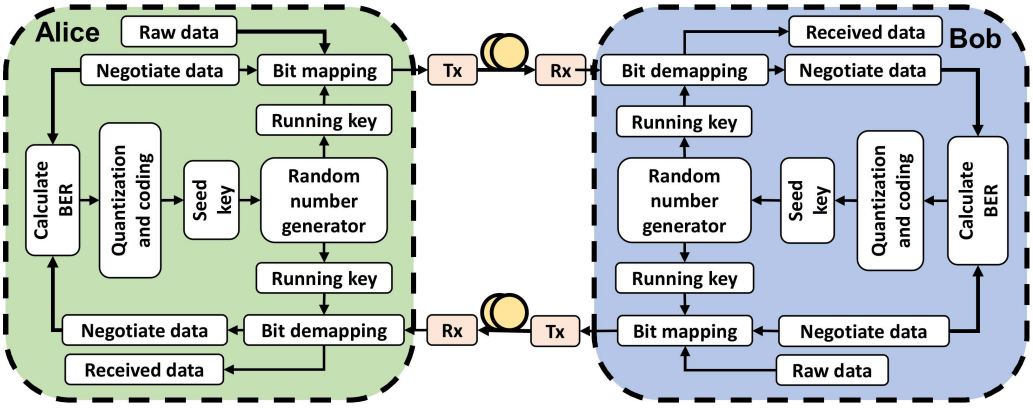

Figure 4. System schematic diagram of QNSC and BER-LM.

The specific operation steps of QNSC and BER-LM are shown in Figure 5:

- Step 1: the locally randomly generated negotiation data and the original data are mapped with the key and sent out.
- Step 2: the key is used to demap the received data.
- Step 3: the data obtained from the demapping are mapped again and then returned to the opposite end.
- Step 4: demap the returned data and compare the obtained negotiation data with the locally randomly generated negotiation data to calculate the BER.
- Step 5: obtain a consistent running key based on the calculated BER.

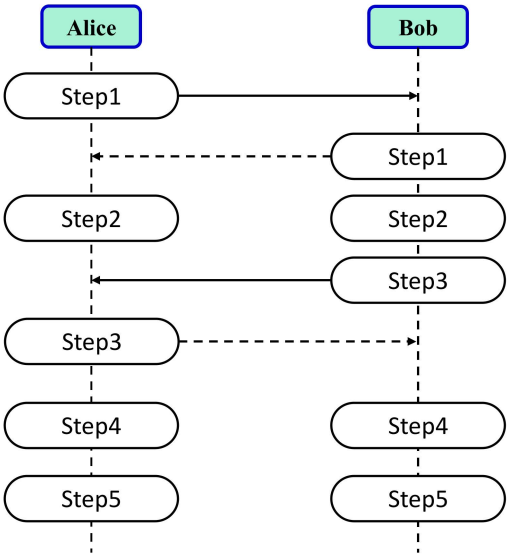

Figure 5. The specific operation steps of QNSC and BER-LM.

This integrated system of QNSC and BER-LM can realize data encryption and key distribution simultaneously in the same fiber channel. It not only saves equipment costs but also makes full use of spectrum resources, which is suitable for large-scale popularization.

The system device diagram of a loopback optical fiber channel is shown in Figure 6. A 1550 nm laser is used, and the data are generated by the digital signal processing (DSP) module at the sending end. DSP includes a series of processes and algorithms such as analog-to-digital and digital-to-analog conversion, dispersion compensation, frequency offset compensation, clock synchronization, channel equalization, carrier phase recovery,

QNSC, etc. [20]. After the IQ modulator, the signal arrives at the variable optical attenuator (VOA) and is amplified by an erbium-doped fiber amplifier (EDFA) before entering the fiber channel. At the Bob side, the signal is amplified by EDFA and enters the coherent optical receiver. The DSP module at the Bob side restores the encrypted signal to the original data and negotiation data. The negotiation data are further processed to obtain the key. Figure 6 shows the received PSK/QNSC signal and the decrypted QPSK signal.

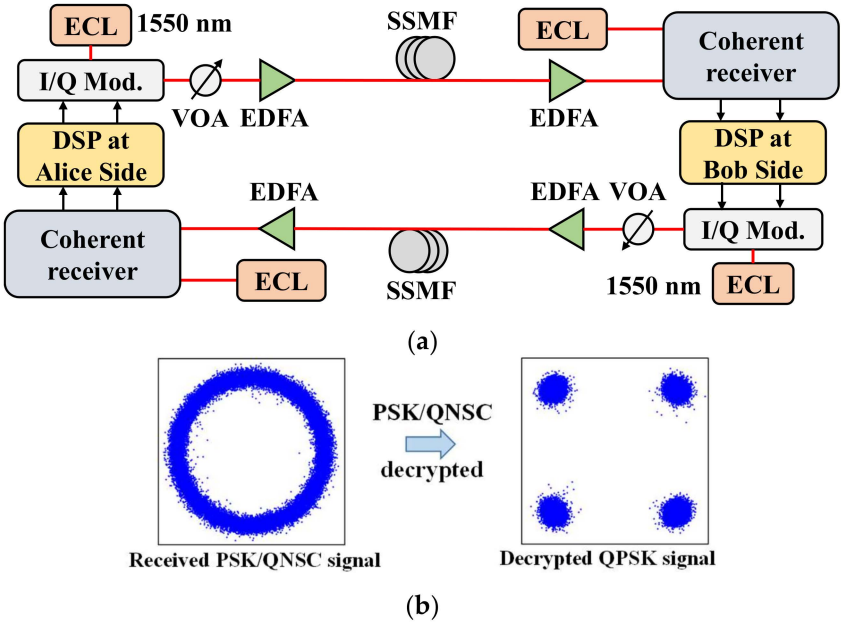

Figure 6. (**a**) System device diagram of loopback optical fiber channel. (**b**) Received PSK/QNSC signal and decrypted QPSK signal.

4. Results and Analysis

First, we studied the encrypted transmission performance of a PSK/QNSC system. Figure 7 shows the signal Q-factor at different transmission distances with and without PSK/QNSC. As the transmission distance increased from 10 km to 200 km, the Q-factor with and without QNSC decreased gradually. When the transmission distance increased to 200 km, the Q factor decreased to the 7% FEC limit. At the same time, it was found that the transmission performance with PSK/QNSC was lower than that without QNSC. When the transmission distance was 100 km, the Q-factor with QNSC was about 1.7 dB lower than that without QNSC. This shows that QNSC gained system security at the cost of losing part of the transmission performance. When the transmission distance was less than 200 km, this cost was worthwhile because correct data could be recovered through FEC. Figure 7 compares three QNSC schemes with modulation formats of 1024 × 1024 PSK, 512 × 512 PSK, and 256 × 256 PSK. With the increase in OSNR, the detection error probability (DFP) of Eve decreased. DFP refers to the probability that Eve could obtain the correct data bit by analyzing the stolen optical signal. This is because, with the increase in OSNR, the masking effect of the noise signal decreased, which made it easier for Eve to obtain the correct data bits. When the OSNR was 30 dB, the DFPs corresponding to the three QNSC schemes were 0.999, 0.998, and 0.994, respectively. This indicates that the higher the modulation order of the PSK signal, the higher the security of the data. This is because with the increase in the modulation order of the PSK signal, the distance between the adjacent constellation points was closer, which made it easier to be masked by noise.

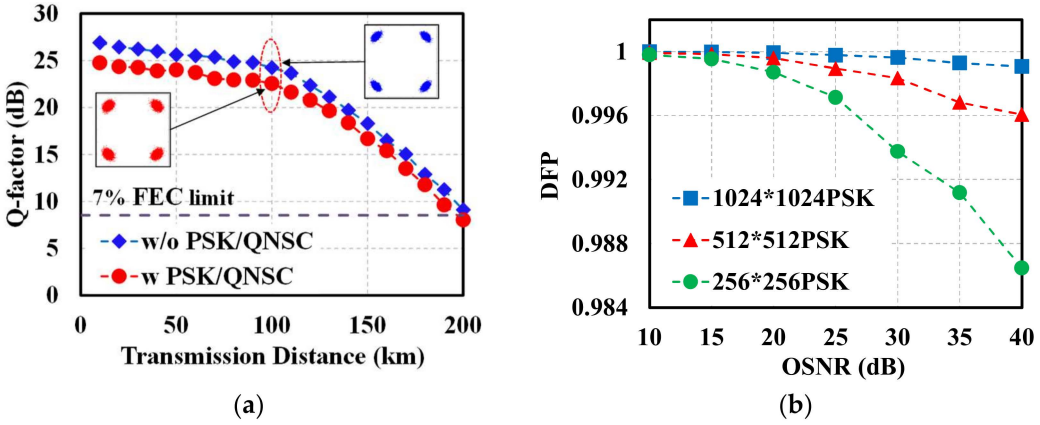

Figure 7. (**a**) Q-factor vs. distance for PSK/QNSC and regular QPSK without PSK/QNSC. (**b**) DFP vs. OSNR for Eve at different OSNR values with encrypted signals of 220PSK, 218PSK, and 216PSK.

Next, we analyzed the key distribution system based on BER-LM. Figure 8 shows the loopback channel BER samples measured by Alice, Bob, and Eve using negotiation bits. It was found that the BER measured by Alice and Bob ranged from 0.25 to 0.3, and their trends were very consistent. However, the BER measured by Eve was concentrated between 0.4 and 0.45, and the BER change trend was different from that of Alice and Bob. This was because the measurement position of Eve was different from that of Alice and Bob. Alice and Bob could measure the BER change of the entire optical fiber channel. However, Eve could only obtain signals from optical fiber lines through light splitting, so the BER of the intercepted signals was high, and the change trend was different from that of the legitimate sender and receiver. Thus, the security of key distribution was guaranteed.

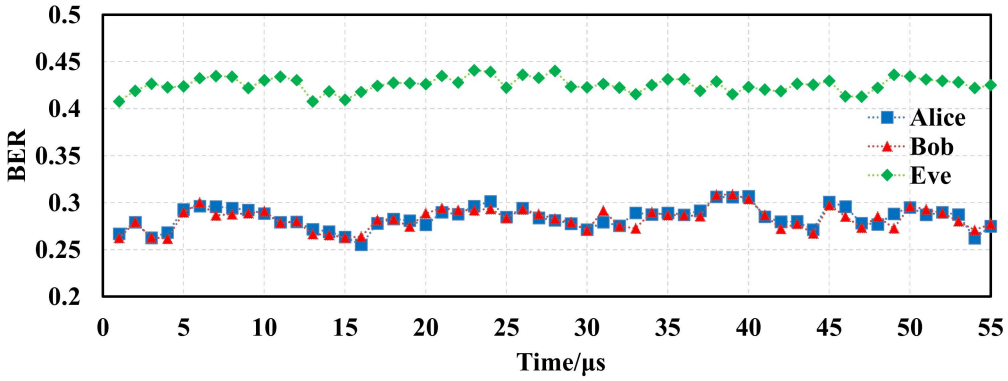

Figure 8. BER measured by Alice, Bob, and Eve at different time points.

Finally, we studied the performance of the QNSC and key joint distribution system. As shown in Figure 9, the Q-factor decreased with an increase in the negotiation bit position. This was because the closer the negotiation data were to the raw data, the more serious the impact on the raw data, resulting in a decline in transmission performance. As shown in Figure 9, as the negotiated bit position increased, the loopback channel BER measured according to the negotiation data gradually decreased. This was because the higher the negotiation bit, the greater the signal amplitude, and the lower the impact of noise, and the lower the BER. As the negotiated bit position decreases, the BER measured by Bob and Eve tends to 0.5, which reduces the security of key distribution. Therefore, in order to ensure that the Q-factor is high enough, the negotiation bit position should be reduced. In order to increase the security of the negotiation key, the negotiation bit position should be improved. We finally chose a negotiated bit position of seven, which can not only ensure that the Q-factor meets the 7% FET limit but also ensures the security of key distribution.

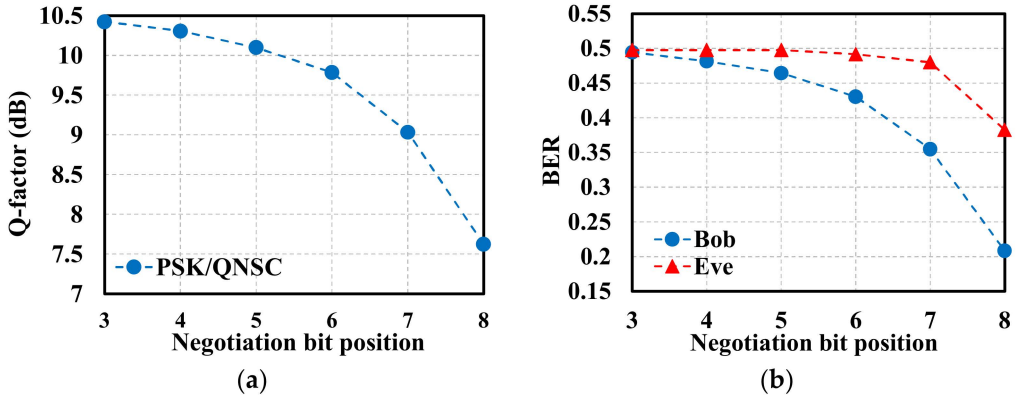

Figure 9. (**a**) Q-factor vs. bit position. (**b**) BER measured by Bob and Eve at different bit positions.

The method presented in this paper has the following advantages. This method does not require the use of a key provided by a third party. This method can provide a self-sufficient key for encrypted transmission. On the basis of the encrypted transmission system, this method only needs to improve the DSP algorithm without adding additional equipment overhead, which reduces the equipment cost and is conducive to large-scale popularization. At the same time, this method also has some limitations. Since the raw data and negotiation data are modulated into the same fiber channel at the same time, the negotiation data will interfere with the raw data, causing the Q-factor of the raw data to decrease. In order to reduce the interference of the negotiation data in the raw data, it is necessary to reasonably set the negotiation bit position. When the negotiated bit position was set to seven, the Q-factor of the signal of the 20 Gpsk, 200 km transaction system was nine, meeting the requirement of the 7% FEC limit.

5. Conclusions

In previous studies, encryption and key distribution were carried out in independent channels. This paper proposes a scheme that combines the two technologies of encryption and key distribution in a single fiber channel. The simulation results show that by reasonably setting the negotiated bit position of key distribution, better security of key distribution can be achieved while ensuring the transmission performance. When the negotiated bit position was seven, the Q-factor of the 20 Gbps coherent transmission system was nine, meeting the 7% FEC limit. This scheme does not require a secure key provided by a third party. This scheme can provide a self-sufficient secure key for data encryption. On the basis of the encrypted transmission system, this scheme only needs to improve the DSP algorithm without adding additional expensive optical equipment, which reduces equipment costs and is conducive to large-scale popularization.

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

Funding: Funding: This research work was supported by the Special Fund of Advantageous and Characteristic disciplines (Group) of Hubei Province. This research work was supported in part by BIGC Project (Ec202201); The Initial Funding for the Doctoral Program of BIGC (27170122006). This research work was supported in part by Scientific Research Project of Fuyang Normal University (2022KYQD0004) and Key scientific research project of Universities in 2021 (KJ2021A0897), Anhui Education Department. This research work was supported in part by Guiding project of Scientific Research Plan of Education Department of Hubei Province (B2022338), and by University Natural Science Research Project of Anhui Province (Grant No.: 2022AH051338). This research work was supported in part by University-level Natural Youth Funding Project of West Anhui University (Project No.: WXZR201907).

Data Availability Statement: This study does not report any data.

Acknowledgments: We acknowledge the support given by Minchen Cai and Shali Wang during this project.

Conflicts of Interest: The authors declare no conflict of interest. The funders had no role in the design of the study; in the collection, analysis, or interpretation of data; in the writing of the manuscript; or in the decision to publish the results.

References

1. Futami, F.; Tanizawa, K.; Kato, K.; Hirota, O. Experimental investigation of security parameters of Y-00 quantum stream cipher transceiver with randomization technique: Part I. *Quantum Commun. Quantum Imaging XV* **2017**, *10409*, 104090I.
2. Futami, F.; Kurosu, T.; Tanizawa, K.; Kato, K.; Suda, S.; Namiki, S. Dynamic routing of Y-00 quantum stream cipher in field-deployed dynamic optical path network. In Proceedings of the Optical Fiber Communication Conference, San Diego, CA, USA, 11–15 March 2018.
3. Tanizawa, K.; Fumio, F. 2^{14} (=16,384) Level Intensity Modulation at 10 Gbaud for Y-00 Quantum Stream Cipher. In Proceedings of the CLEO: QELS_Fundamental Science, San Jose, CA, USA, 13–18 May 2018.
4. Tanizawa, K.; Fumio, F. 2^{14} Intensity-Level 10-Gbaud Y-00 Quantum Stream Cipher Enabled by Coarse-to-Fine Modulation. *IEEE Photonics Technol. Lett.* **2018**, *30*, 1987–1990. [CrossRef]
5. Tanizawa, K.; Fumio, F. Digital Coherent 20-Gbit/s DP-PSK Y-00 Quantum Stream Cipher Transmission over 800-km SSMF. In Proceedings of the Optical Fiber Communication Conference, San Diego, CA, USA, 3–7 March 2019.
6. Tanizawa, K.; Fumio, F. Digital-coherent PSK Y-00 quantum stream cipher for secure fiber-optic transmission. *Metro Data Cent. Opt. Netw. Short-Reach. Links II* **2019**, *10946*, 109460B.
7. Tanizawa, K.; Fumio, F. Digital coherent PSK Y-00 quantum stream cipher with 217 randomized phase levels. *Opt. Express* **2019**, *27*, 1071–1079. [CrossRef] [PubMed]
8. Wang, X.; Li, Y.; Zhao, Y.; Lei, C.; Zhang, H.; Zhang, J. Physical layer authentication based on BER measurement of optical fiber channel. *IEEE Access* **2020**, *8*, 101812–101823. [CrossRef]
9. Wang, X.; Zhang, J.; Wang, B.; Zhu, K.; Song, H.; Li, R.; Zhang, F. Key Distribution Scheme for Optical Fiber Channel Based on SNR Feature Measurement. *Photonics* **2021**, *8*, 208. [CrossRef]
10. Zaman, I.U.; Lopez, A.B.; Al Faruque, M.A.; Boyraz, O. Polarization mode dispersion-based physical layer key generation for optical fiber link security. In Proceedings of the Novel Optical Materials and Applications, New Orleans, LA, USA, 24–27 July 2017.
11. Scheuer, J.; Kotlicki, O. Dark states ultra-long fiber laser (UFL) for practically secure key distribution. In Proceedings of the Asia Communications and Photonics Conference, Beijing, China, 12–15 November 2013.
12. Bar-Lev, D.; Scheuer, J. Enhanced key-establishing rates and efficiencies in fiber laser key distribution systems. *Phys. Lett. A* **2009**, *373*, 4287–4296. [CrossRef]
13. Zadok, A.; Scheuer, J.; Sendowski, J.; Yariv, A. Secure key generation using an ultra-long fiber laser: Transient analysis and experiment. *Opt. Express* **2008**, *16*, 16680–16690. [CrossRef] [PubMed]
14. Kotlicki, O.; Scheuer, J. Secure key distribution over a 200 km long link employing a novel ultra-long fiber lasers (ufl) scheme. In Proceedings of the Conference on Lasers and Electro-Optics: Applications, San Jose, CA, USA, 16–21 May 2010.
15. El-Taher, A.; Kotlicki, O.; Harper, P.; Turitsyn, S.; Scheuer, J. Secure key distribution over a 500 km long link using a Raman ultra-long fiber laser. *Laser Photonics Rev.* **2014**, *8*, 436–442. [CrossRef]
16. Marand, C.; Paul, D.T. Quantum key distribution over distances as long as 30 km. *Opt. Lett.* **1995**, *20*, 1695–1697. [CrossRef] [PubMed]
17. Hughes, R.J.; Morgan, G.L.; Peterson, C.G. Quantum key distribution over a 48 km optical fibre network. *J. Mod. Opt.* **2000**, *47*, 533–547. [CrossRef]
18. Tanaka, A.; Fujiwara, M.; Nam, S.W.; Nambu, Y.; Takahashi, S.; Maeda, W.; Yoshino, K.-I.; Miki, S.; Baek, B.; Wang, Z.; et al. Ultra fast quantum key distribution over a 97 km installed telecom fiber with wavelength division multiplexing clock synchronization. *Opt. Express* **2008**, *16*, 11354–11360. [CrossRef] [PubMed]
19. Yuen, H.P. KCQ: A new approach to quantum cryptography I. General principles and key generation. *arXiv* **2003**, arXiv:quant-ph/0311061.
20. 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]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.