Long-haul and High-speed Key Distribution Based on One-way Non-dual Arbitrary Basis Transformation in Optical Fiber Link

Chao Lei, Jie Zhang*, Yajie Li, Yongli Zhao, Bo Wang, Hang Gao, Junjia Li, Mingrui Zhang
State Key Laboratory of Information Photonics and Optical Communications
Beijing University of Posts and Telecommunications, Beijing, 100876, China
** jie.zhang@bupt.edu.cn*

Abstract: We propose a long-haul and high-speed key distribution based on one-way non-dual arbitrary basis transformation in optical fiber link. The key distribution rate of 277 Kbit/s with free key error rate is demonstrated over 300km.

1. Introduction

Secure key distribution has been considered as a substantial problem in security schemes [1]. Currently, in the field of optical communication, quantum key distribution (QKD) has been widely studied as an alternative technique to provide unconditional security, but the implementation of QKD increases the cost and complexity of system design [2]. Therefore, recent research focuses on how to realize key distribution with low cost and high system compatibility. For example, several schemes have been proposed to achieve error-free secure key distribution, including polarization mode dispersion (PMD)-based in the physical layer [3] and exploiting Stokes parameters (SPs) of the state of polarization [4]. Besides, there are some other methods, including using Mach-Zehnder interferometer (MZI) covering the entire distance between the communicating parties [5] and phase fluctuation of orthogonal polarization modes (OPM) in optical fiber channel [6].

However, in terms of key distribution rate (KDR), the highest KDR of the above methods is 500bit/s [3]. The longest transmission distance L of these schemes is less than 60km. In addition, these methods will change the structure of an optical communication node, which is incompatible with the existing transmission systems. Therefore, it is still significant to explore a long-haul and high-speed security key distribution scheme with low cost and high compatibility.

In this paper, we propose a long-haul and high-speed secret key distribution based on asymmetric basis Y-00 protocol in optical fiber link. The proposed secure key distribution is based on analyzing the bit error rate (BER) between transmitted data and received data of Alice. The variation of BER is caused by one-way non-dual arbitrary basis transformation (ONABT). The experiment demonstrates that this key distribution scheme is feasible and the KDR can reach up to 277 Kbit/s with free key error rate (KER) over 300km standard single-mode fiber (SSMF). Then, the NIST test suite is employed to evaluate the randomness of the obtained secret keys. Besides, the security of the proposed scheme is evaluated in the case of a fiber-tapping attack. Since digital signal processor (DSP) distributes the keys, the scheme is compatible with the current optical transmission system without changing node structure.

2. PRINCIPLE OF SECURE KEY DISTRIBUTION BASED ON ONABT

Fig. 1 shows the flow-process diagram of the key distribution scheme based on ONABT. D_{AT} , D_{AR} and B_A means transmission data, receive data and basis state in Alice respectively, which are generated by pseudo-random number generator (PRNG). In the Y-00 Encryption/Decryption module, we transmit/receive 1024*1024QAM/DFTs-OFDM signals with a bit rate of 10Gbit/s for encryption and decryption using a low bit (such as 7bit not 10bit in-phase/quadrature (I/Q)) [7], $B_A(1)$ is the lowest bit of B_A . In addition, the transmission distance between Alice and Bob can reach 300km.

On the side of Bob, D_{BT} , D_{BR} and B_B means transmission data, receive data and basis state in Bob respectively, which also generated by PRNG. D_S is generated by PRNG. It is worth noting that B_A and B_B are independent random variables. D_S is the key of Bob. D_{Ex} is expansion data of D_S . For example, D_S = {…110010…}, D_{Ex} = {…111111000000111000…} with expansion factor λ equal to three. Alice calculates the data BER by using the extension factor λ on the Bob side. According to the calculated BER curve, Alice uses the formula (1) to quantize and decide to obtain the key of Alice. $Q(\lambda)$ of Alice has a large difference between D_{Ex} = {…111…} and D_{Ex} = {…000…}, which means the data expanded on the Bob side can be transformed to Alice. Moreover, after quantification and decision of $Q(\lambda)$, Alice can obtain the same key as Bob.

$Q(\lambda)$ is a sequence of Alice's BER curve, $F(\lambda)$ is a key sequence of Alice, α is a scalar.

$$F(\lambda)=\begin{cases}1 & if \quad Q(\lambda)\geq T_{+}\\ 0 & if \quad Q(\lambda)\leq T_{-}\end{cases} \qquad T_{\pm}=\text{mean}\pm\alpha\times\text{variance} \tag{1}$$

In summary, the "O" of the ONABT scheme indicates that the unidirectionality of Alice transmission and reception. The "NAB" of the ONABT scheme indicates that Alice and Bob have a relatively independent randomly generated basis respectively. The "T" of the ONABT scheme means that Bob will XOR the D_{Ex} and D_{BR} to generate D_{BT}. Using the proposed ONABT scheme, Bob can distribute the key D_S to Alice.

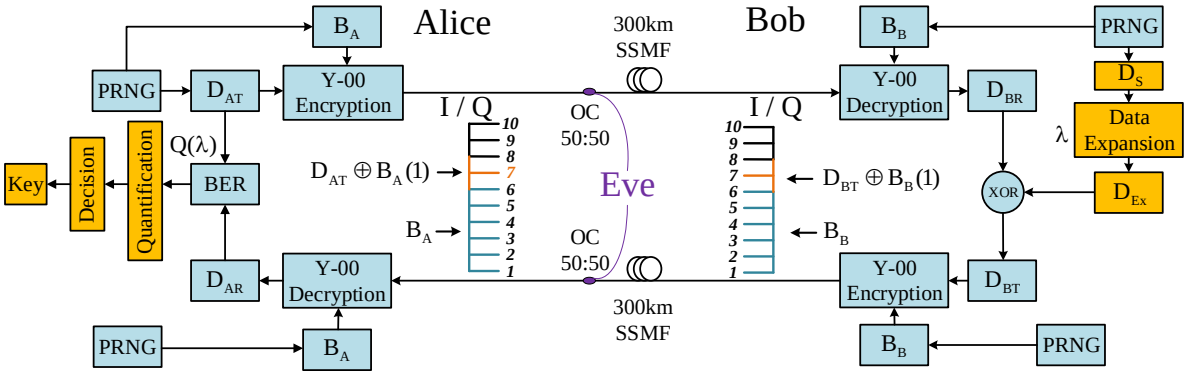

Fig. 1. Secure key distribution scheme.

3. Experimental setup and results analysis

We conduct a key distribution experiment over 300km SSMF. The photograph of the experiment platform for key distribution is shown in Fig. 2. At the transmitter, an external cavity laser (ECL) sends a beam at 1550nm with 10dBm power into an I/Q modulator. In the DSP of the transmitter, D_{AT} is generated by PRNG. After Y-00 encryption, the I and Q data are converted by an arbitrary waveform generator (AWG) to an electrical signal at the sampling rate of 10-GSa/s. After amplified by the Modulator Driver (MD), the signal is loaded onto the light carrier by an I/Q modulator. Then, the signal is amplified by an erbium-doped fiber amplifier (EDFA) and propagated through a 300km SSMF to distribute the key. Each part is amplified by an EDFA at the receiver side and detected by a coherent optical receiver combined with an ECL local- oscillator (OL). The detected I/Q signals are then captured by a 40-GSa/s real-time oscilloscope.

Fig. 2. Photograph of experiment platform for key distribution.

As shown in Fig. 3(a), in the optical back-to-back (OBTB) condition, the Red line represents the $Q(\lambda)$ of Alice when D_{Ex} = {…000…}, the Blue line represents the $Q(\lambda)$ of Alice when D_{Ex} = {…111…} respectively. This means that Bob transmits D_{BR} and $\bar{D}_{BR}$ to Alice, causing Alice's BER to be different. The difference in BER can be exploited to transmit information. The results in Fig. 3(a) confirm that the principle of the ONABT scheme in section 2.

In Fig. 3(b), the KER between Alice and Bob decreases with the increase of λ. It is worth noting that in the case of L is 300km, KER equal to zero when λ is 3600. The comparison of the proposed scheme with other key distribution schemes using MZI, OPM and SPs in terms of KDR, KER and L are given in Fig. 3(c). In our scheme, we provide not only an alternative key distribution approach but also long-haul crossed over 300km fiber.

In addition, to evaluate the randomness of the obtained secret keys, the NIST test suite is employed, where all of the 15 indexes were implemented using a key sequence with a length of 10^6. If the P-value>0.01 of each index of the NIST test, the sequence can ensure randomness. Table 1 shows the final results of the tests. All of the 15 indexes have been passed, which confirms the randomness of the distributed key in the proposed ONABT scheme.

An attack method is described to verify the security of the distributed keys. It should be mentioned that Bob transmits D_{BR} and $\bar{D}_{BR}$ to Alice, causing Alice's BER to be different. Due to the increase of λ (such as λ from 200 to 3600), this difference of BER increases. Therefore, the security brought by noise will decrease. when λ is 3600, although the KER equal to zero, the security performance is lower than that with small λ. Besides, since Eve uses a 50:50 optic coupler (OC), this condition brings more information to Eve than normal condition 99:1 OC. The KER between Eve and Bob we measured is 0.25 with λ is 3600, which fits the above analysis.

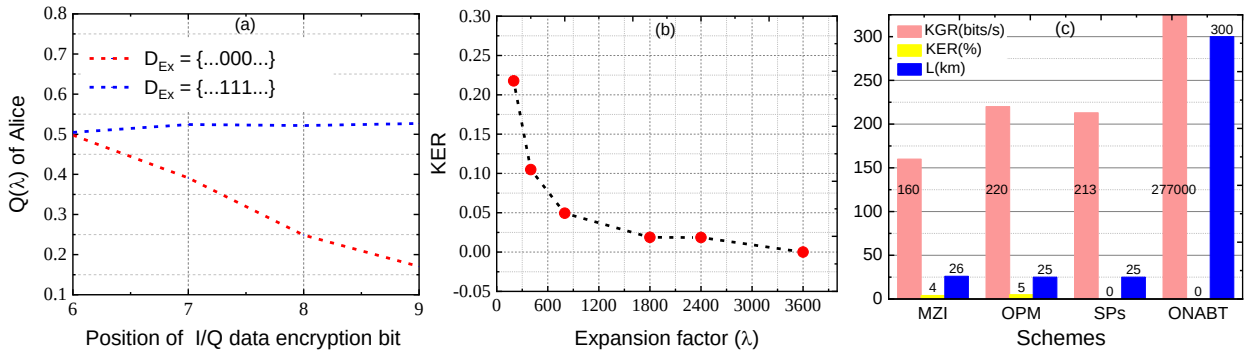

Fig. 3. (a) BER of Alice (b) KER between Alice and Bob (c) Performance comparison of different schemes

Table 1. Results of the 15 NIST tests.

Index	***P-value***	***Index***	***P-value***
Approximate entropy	0.263399	Overlapping Template	0.407310
Block frequency	0.873946	Random Excursions (data1)	0.203812
Cumulative sum (Forward/Reverse)	0.957206/0.621010	Rank	0.517667
FFT	0.110325	Runs	0.421228
Frequency	0.589197	Serial (data1)	0.747032
Linear Complexity	0.803519	Universal	0.997937
Longest Run	0.434071	Random ExcursionsVariant (data1)	0.014688
Non-Overlapping Template (data1)	0.510756		

4. Conclusions

In this paper, we propose a long-haul and high-speed key distribution scheme based on ONABT in the optical fiber link. The experiment results reveal that the KDR of 277 Kbit/s with free KER is successfully demonstrated when λ is 3600. The proposed scheme can achieve secure key distribution over 300 km SSMF, which is much longer than the existing MZI, OPM and SPs schemes. Moreover, due to distributing key by DSP, the scheme is compatible with the current optical transmission system without changing node structure. In the future work, the ONABT scheme can integrate with quantum noise stream cipher transmission system to further reduce costs and improve system compatibility.

Acknowledgment This work was supported in part by NSFC Projects (Grant No. 61831003, 61901053, 61822105).

References

[1] K. Jonathan, et al., Introduction to Modern Cryptography, 2nd ed.New York, NY, USA: Chapman & Hall, 2014.
[2] Gisin, Nicolas, et al., "Quantum cryptography." Reviews of modern physics, 74(1), 145 (2002).
[3] Zaman, Imam Uz, et al., "Polarization mode dispersion-based physical layer key generation for optical fiber link security." Optical Sensors. Optical Society of America, JTu4A-20 (2017).
[4] Zhang, Liuming, et al., "Error-free secure key generation and distribution using dynamic Stokes parameters." Optics Express, vol. 27, 29207-29216 (2019).
[5] Kravtsov, Konstantin, et al., "Physical layer secret key generation for fiber-optical networks." Optics Express, vol. 21, 23756-23771 (2013).
[6] Hajomer, Adnan AE, et al., "Key distribution based on phase fluctuation between polarization modes in optical channel." IEEE Photonics Technology Letters, vol. 30, 704-707 (2018).
[7]Yang, Xiaokun, et al., "Demonstration of Key Generation Scheme Based on Feature Extraction of Optical Fiber Channel." ACP.1-3, (2018).