CHALMERS
UNIVERSITY OF TECHNOLOGY

Integration of Self-Adaptive Physical-Layer Key Distribution and Encryption in Optical Coherent Communication

Citation for the original published paper (version of record):
Chao, L., Lin, R., Li, Y. et al (2023). Integration of Self-Adaptive Physical-Layer Key Distribution and Encryption in Optical Coherent
Communication. Journal of Lightwave Technology, 41(17): 5599-5606.
http://dx.doi.org/10.1109/JLT.2023.3257963

This article has been accepted for publication in IEEE/OSA Journal of Lightwave Technology. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/JLT.2023.3257963

Integration of Self-Adaptive Physical-Layer Key Distribution and Encryption in Optical Coherent Communication

Chao Lei, Rui Lin, Yajie Li, Bo Wang, Mingrui Zhang, Yongli Zhao, and Jie Zhang

***Abstract*— We propose and experimentally demonstrate a compatible physical-layer secure optical communication (PLSOC) system that integrates self-adaptive physical-layer key distribution (PLKD) and encryption (PLE) in optical coherent communication. Based on bit error rate difference of QAM signals mapped by asymmetric basis state Y-00 protocol, the secret key can be secretly exchanged over public fiber links without the pre-shared keys. Moreover, we perform a parameter self-adaptive strategy for practical and dynamic PLKD. The security of the key is evaluated in the case of a fiber-tapping attack. A secure hash algorithm, SHA3-512, is used to perform privacy amplification to obtain the virtually secure key. An error-free PLKD rate reaches 39.3 Kbits/s over 300km ultra-low loss fiber. We experimentally enable the integration of the proposed PLKD scheme and quantum noise stream cipher (QNSC) with a single wavelength, same system. Q factor penalty of the integration system compared to the QNSC system is 3.7dB (optical back-to-back) and 4.8dB (300km) respectively. By exploiting a common hardware platform, with the same wavelength, the proposed PLSOC system addresses the problem that PLKD and PLE are separately performed through independent optical fiber links or wavelengths. Since only digital signal processing is used, the scheme does not require extra hardware.**

***Index Terms*— physical-layer secure optical communication, physical-layer key distribution, physical-layer encryption, Y-00 protocol, quantum noise stream cipher.**

I. Introduction

Over recent decades, internet traffic has been growing tremendously. Optical fiber communication network serves as the infrastructure for carrying massive data, much of which is private, sensitive, or confidential. However, optical fiber is vulnerable to many attacks (e.g., fiber tapping, etc.) [1]. Physical-layer security plays a vital role in the current optical communication system. A physical-layer secure optical communication (PLSOC) system involves physical-layer encryption (PLE) and physical-layer key distribution (PLKD). The purpose of PLE is to hide the plain text signals in random or pseudo-random signals in various ways. One promising PLE scheme is the quantum noise stream cipher (QNSC), also known as Y-00 protocol. It hides the plain text signals into the quantum shot noise and amplified spontaneous emission (ASE) noise through an encryption algorithm in the digital domain to enable high-security communication [2]. The transmission rate can achieve 40Gb/s over a 480km transmission distance [3]. Since QNSC can be performed by digital signal processing (DSP), it is compatible with the existing coherent optical communication system. However, pre-shared keys are essential in the QNSC system. The above PLSOC systems generally assume that the key for QNSC-based PLE is already distributed [4], or that PLKD and PLE are separately performed through independent optical fiber links or wavelengths [5]. Extra equipment or spectrum resources impede their compatibility with the current communication systems.

For PLKD, a substantial problem in the security schemes [6], currently in the field of optical communication, quantum key distribution (QKD) has been widely studied as a technique to provide unconditional security. However, the high expense and complexity hinder its massive deployment [7]. Besides, optical chaos derived from a pre-shared chaotic laser system can be utilized as an external wideband entropy source to distribute secure key [8-11]. However, identical devices or privately preset features are needed. In addition, a high-speed chaotic polarization scrambler driven by digital chaos is introduced to achieve the PLKD with a key rate of ~Mbps [12]. A polarization scrambler [13][14] is utilized to alter rapidly and symmetrically the state of polarization for the key rate of ~Gbps. However, the extra random sources make these schemes not widely applied. Briefly, customized hardware is needed in those schemes, which are not compatible with the existing transmission systems.

Furthermore, a fully compatible key generation and distribution scheme can be realized by only using DSP without any extra hardware. For instance, key generation and distribution are realized by using bit error rate (BER) curves based on reciprocity and randomness in the optical channel [15][16] and angular differences in the PSK modulation system

This work was supported in part by National Natural Science Foundation of China (NSFC) Projects (Grant No. 61831003, 61901053, 61822105), and the EUREKA cluster CELTIC-NEXT project AI-NET PROTECT funded by VINNOVA, the Swedish Innovation Agency. (*Corresponding author: Jie Zhang).*

C. Lei, Y. Li, B. Wang, M. Zhang, Y. Zhao, and J. Zhang are with the State Key Laboratory of Information Photonic and Optical Communication (IPOC), Beijing University of Posts and Telecommunications (BUPT), Beijing, 100876, China. (e-mail: chaolei@bupt.edu.cn; yajieli@bupt.edu.cn; wb1059@gmail.com; mingruizhang@bupt.edu.cn; yonglizhao@bupt.edu.cn; jie.zhang@bupt.edu.cn).

R. Lin is with Electrical Engineering Department, Chalmers University of Technology, SE-412 96 Gothenburg, Sweden (e-mail: ruilin@chalmers.se).

using random initial angles [17]. Key distribution using phase noise in uneven PSK modulation system [18] and PSK/QNSC system [19] are also achieved. The key distribution also exploits the difference in the probability of the correct decision of signals in the Y-00 protocol system [20]. Toward a compatible PLOSC system, it is desirable to integrate the PLKD scheme into the QNSC-based PLE scheme using DSP only.

In this paper, we propose a self-adaptive PLKD scheme and its integration with the QNSC-based PLE system. An experiment over a 300km fiber link is carried out for validity purposes. Both the PLKD and the PLE are realized by DSP without any extra hardware on top of the optical coherent communication system. Furthermore, the data used to implement PLKD and PLE are derived from different specific bits of the symbols. In this way, PLKD and PLE can share the same time slot. Comparing the separated PLKD and PLE schemes, the proposed integration system can support more frequent key updates so that a more secure PLOSC system can be obtained.

The remainder of this paper is structured as follows: In Section II, we introduce the proposed PLKD scheme. Firstly, we specify the QAM mapping of asymmetric basis state Y-00 protocol in the PLKD scheme in Part A, and then describe the proposed parameter self-adaptive strategy for the PLKD scheme in Part B. In Section III, we analyze the eavesdropper's difficulties in the case of a fiber-tapping attack and improve the key security using privacy amplification. In Section IV, the integration of the proposed PLKD scheme with the QNSC-based PLE is illustrated for a compatible PLOSC system. The main contribution and results are summarized in Section V.

II. Physical-layer Key Distribution

A. Scheme and Principle

Fig. 1 shows the diagram of the proposed key distribution scheme. A point-to-point optical communication system is used to demonstrate the key distribution principle. We illustrate the scheme in the order of the logical link as shown in Fig. 1.

On Alice's side, D_{AT}, D_{AR}, and B_A denote the transmitted data, the received data, and the basis state respectively. D_{AT}, B_A are generated by a pseudo-random number generator (PRNG). In the QAM Mapping of asymmetric basis state Y-00 protocol module, briefly, the QAM Mapping module (Fig. 2 shows the details of QAM Mapping of asymmetric basis state Y-00 protocol in key distribution), D_{AT} is mapped into high order constellation space using B_A and is transmitted to Bob.

On Bob's side, D_{BT}, D_{BR}, and B_B denote the transmitted data, the received data, and the basis state respectively. B_B is generated by PRNG. It is worth noting that B_A and B_B are independent random bit sequences. D_S is pseudo-random bit sequences (PRBS) generated by PRNG and serves as the key of Bob, KeyB. D_{EX} is the bit sequences by duplicating the bits in D_S. For example, $D_S = \{\ldots 10 \ldots\}$, $D_{EX} = \{\ldots 111000 \ldots\}$ where bit duplication times called λ is three. Bob demaps the signals mapped by Alice using B_B and obtaining D_{BR}. $D_{BT} = D_{BR} \oplus D_{EX}$ is mapped by using the corresponding same basis state B_B as D_{BR} and is transmitted to Alice after bit duplication from D_S to D_{EX}.

Alice receives D_{AR} using the corresponding same basis state B_A as D_{AT}. Then, Alice measures the BER curves between D_{AT} and D_{AR}. The length of the bit sequences for BER calculation is equal to the λ on the Bob side. The λ value is fixed during a key distribution cycle. Alice quantifies the curve and obtains the KeyA, the decision is made according to equation (1). $Q_\lambda(t)$ is Alice's BER value sequences, $F_\lambda(t)$ is the key bit sequences of Alice, and α is a constant ranging from 0 to 1. T_+ and T_- are the upper and lower decision thresholds respectively. *m* and *v* are the mean and variance of $Q_\lambda(t)$ during a key distribution cycle.

Firstly, Alice calculates $T_\pm$ during a key distribution cycle with a certain value α. Second, if one value in $Q_\lambda(t)$ is greater than T_+, Alice decides that the distributed key bit is 1. If one value in $Q_\lambda(t)$ is less than T_-, Alice decides that the distributed key bit is 0. If $Q_\lambda(t)$ is greater than T_- and less than T_+, it is not considered as one correctly distributed key bit.

$$F_\lambda(t)=\begin{cases}1 & if \quad Q_\lambda(t)\ge T_+\\ 0 & if \quad Q_\lambda(t)\le T_-\end{cases} \qquad T_\pm = m \pm \alpha \times v \tag{1}$$

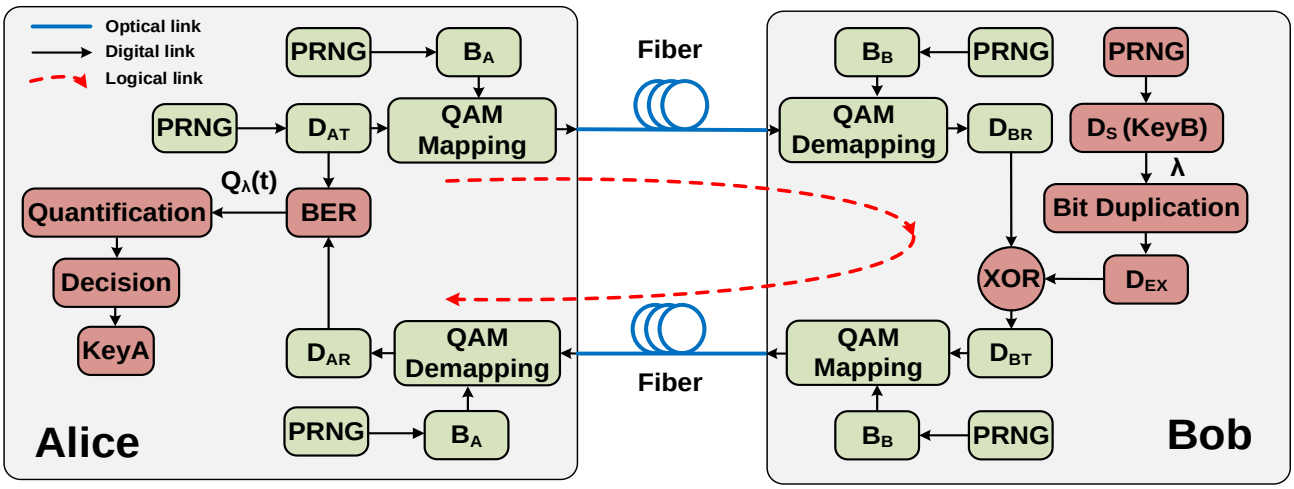

Fig. 1. The diagram of the proposed key distribution scheme

Fig. 2 shows the QAM Mapping of asymmetric basis state Y-00 protocol in the key distribution scheme (mapping of Y-00 the protocol is shown in [21]). There are two significant differences between the asymmetric basis state Y-00 and Y-00 protocol. The first is that legitimate parties don't share the same secret seed keys in the asymmetric basis state Y-00 protocol comparing Y-00 protocol needed pre-shared keys. The second is that data at the bit position of the symbol operated in the Y-00 protocol should be error-free after transmission, masked for security in asymmetric basis state Y-00 protocol and it's not error-free. In [15][16], legal parts need the same basis state for the first-round feature extraction which is not reasonable since it leaves a loophole for the key distribution. In the proposed scheme, keys are generated in one legal part already. The system utilizes noise to mask the keys and stealthily distribute keys from one to another legal part. The scheme uses the random basis state for key distribution which can truly achieve secure keys exchange between legitimate users without any pre-shared basis states. The following is a detailed description of the asymmetric basis state Y-00 protocol.

At the transmitter, Alice drives three PRNGs (e.g., linear feedback shift registers). One is for the random bit pattern for the 1st basis state R_I (upper 1 bit) and R_Q (lower 1 bit) for the first exclusive-OR(XOR) operation of the In-phase (I) channel and Quadrature-phase (Q) channel data, and the second one is a random pattern for other basis states B_I (upper x + y bits) and B_Q (lower x + y bits) for I and Q, respectively. Measurement data (MD), which is derived by the third PRNG, for key distribution (2 bits/symbol) are separated into S_I (upper 1 bit) and S_Q (lower 1 bit). In both cases, a serial-to-parallel conversion technique is used for I and Q data. The encrypted I and Q data are given by the mapped (I, Q) data = $(S_I \oplus R_I + B_{Ix} + B_{Iy},\ S_Q \oplus R_Q + B_{Qx} + B_{Qy})$. B_{Ix}, B_{Iy} are the x bits and y bits basis states from B_I. B_{Qx}, B_{Qy} are the x bits and y bits basis states from B_Q. The (y+1)th bit position that operated $S_I \oplus R_I, S_Q \oplus R_Q$ is the bit position of MD in one symbol. The

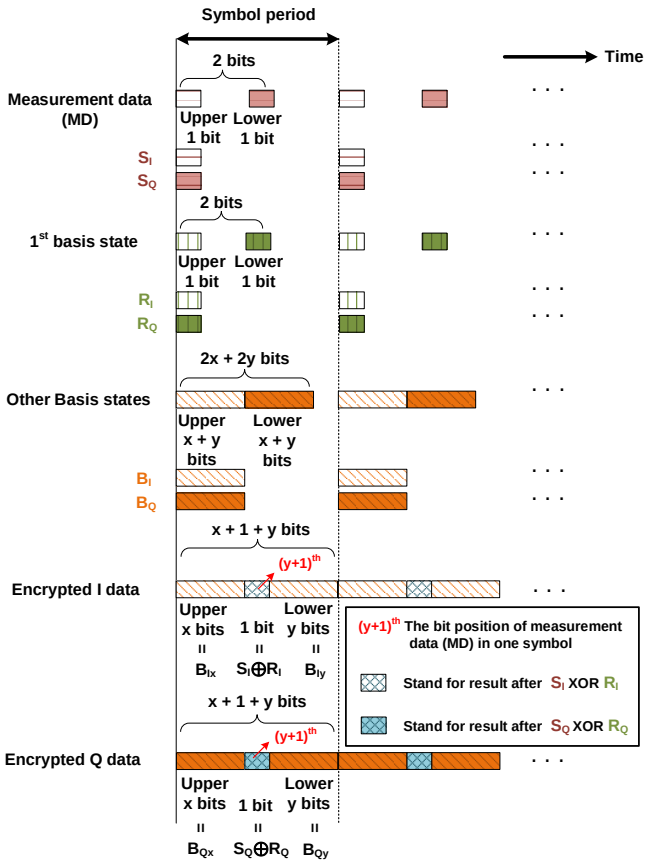

Fig. 2. QAM Mapping of asymmetric basis state Y-00 protocol in key distribution.

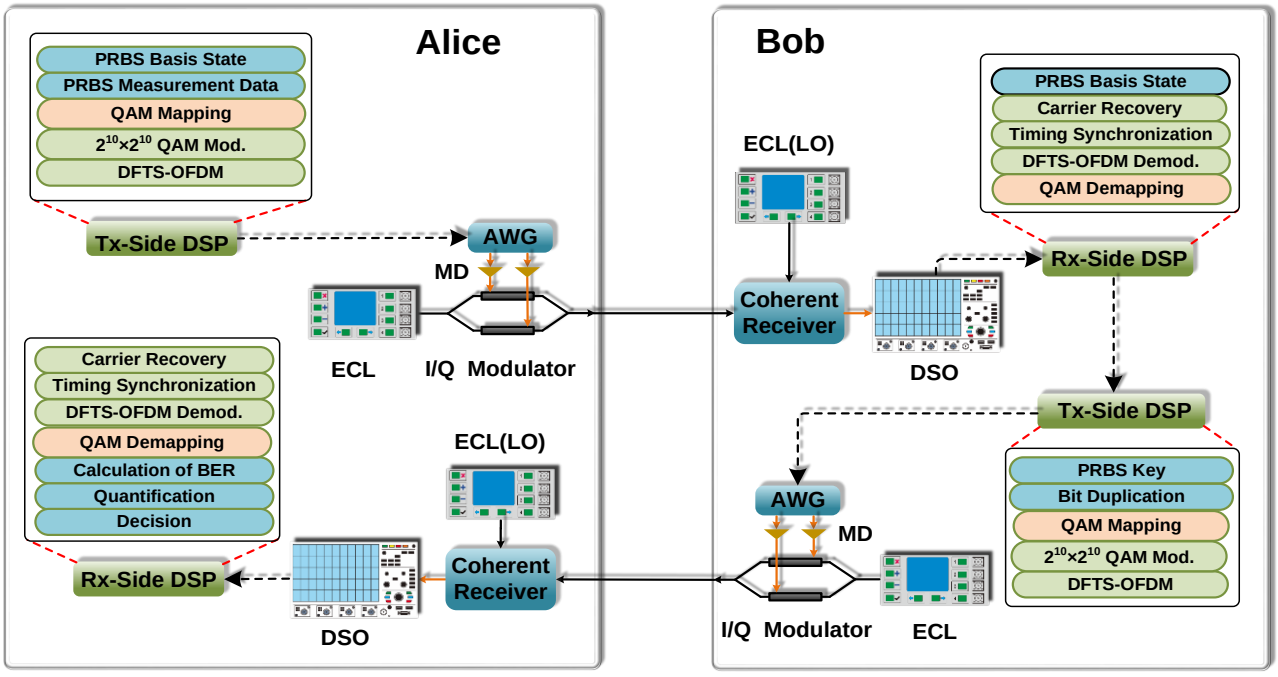

Fig. 3. Key distribution experiment with the optical back-to-back configuration. ECL: External Cavity Laser; MD: Modulator Driver; AWG: Arbitrary Waveform Generator; LO: Local-oscillator; DSO: Digital Storage Oscilloscope; DFTs-OFDM: Discrete Fourier Transform Spread Orthogonal Frequency Division Multiplexing.

This article has been accepted for publication in IEEE/OSA Journal of Lightwave Technology. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/JLT.2023.3257963

length of the encrypted I and Q data is M, $M = x + y + 1$. After performing the QAM mapping with asymmetric basis state Y-00 protocol, a $2^M \times 2^M$ multi-level modulation signal can be obtained. To demonstrate the feasibility of the proposed key distribution scheme, we experiment with the optical back-to-back configuration as shown in Fig.3. Alice and Bob have the same transmitter and receiver.

At the transmitter, an external cavity laser (ECL) sends a beam at 1550nm with 10dBm power into an I/Q modulator. In the QAM mapping module, the encrypted signal is divided into 2 bands after encryption mapping. Each band of data is converted to the frequency domain by applying a 256-point discrete Fourier transform (DFT). The two bands are inserted in the center of the transmitter bandwidth. Some subcarriers around zero frequency called guard interval are reserved. The guard interval is 40 subcarriers in this case. By padding zeroes on the higher frequency part, a 1024-point inverse discrete Fourier transform (IDFT) is used to generate the DFTS-OFDM signal. The neglected high-frequency part includes 472 (1024-512-40) subcarriers. The cyclic prefix size is 32. The subcarrier spacing is 9.765625 MHz (10G/1024). x and y are equal to 3 and 6 separately in this case, the $2^{10}\times2^{10}$ QAM/DFTs-OFDM encrypted signals are converted by an arbitrary waveform generator (AWG) to the electrical domain at the sampling rate of 10 Gsa/s. The transmitter directly connects with the receiver. The encrypted signals are detected by a coherent optical receiver combined with an ECL local oscillator (LO). The detected I/Q signals are then captured by a 40 Gsa/s real-time digital storage oscilloscope (DSO). In terms of parameters, we set α to zero, which simplifies the verification step and prevents repeating the verification step because the non-zero α cannot get a consistent key all the time. λ is equal to 64800, namely the length of one frame of signals. Such one frame carries one key bit for simplifying analysis. D_{AT}, B_A, B_B, and D_S are generated by PRNG in MATLAB.

The experimental result is shown in Fig. 4, the BER values of Alice (namely $Q_\lambda(t)$) are a function of the bit position of MD (namely ρ). The red line represents the BER values of Alice when $D_{EX} = \{\ldots000\ldots\}$ means Bob distributes the key of 0. The blue line represents the BER of Alice when $D_{EX} = \{\ldots111\ldots\}$ means Bob distributes the key of 1. It indicates that Alice can extract the key distributed by Bob utilizing the BER difference

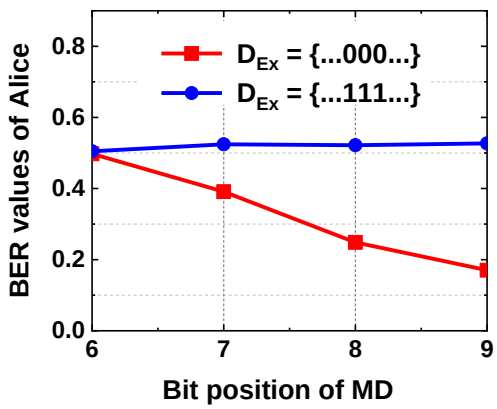

Fig. 4. BER value of Alice as a function of bit position of MD

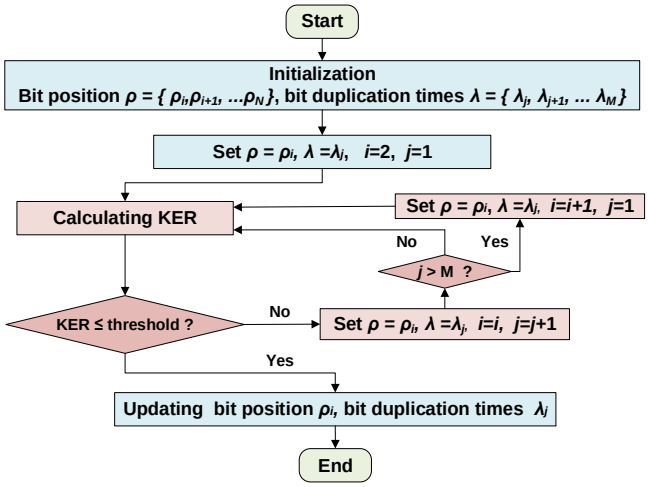

Fig. 5. The flow chart of parameter self-adaptive strategy in key distribution.

of signals. Therefore, it's feasible that the BER difference using asymmetric basis state Y-00 protocol can be exploited for key distribution and extraction in the optical fiber communication system.

B. *Parameter Self-Adaptive Strategy*

Key security (KS), key distribution rate (KDR), and key error rate (KER) are vital performance indicators of the PLKD system. From the KS aspect, as shown in Fig.4, the closer between the BER of key 0 and key 1 (red and blue curves), the more difficult it is to correctly distinguish between 0 and 1 of the distributed keys. The security of the proposed scheme comes from the noise in the link, including quantum noise of the laser and ASE noise, which can mask the MD and basis state difference between the legal parties and the eavesdropper. According to [22], the lower ρ leads to a higher difficulty in decision-making for receiving data, and therefore enhanced security can be achieved. Moreover, as λ increases, the KS decreases. It is because the eavesdropper can get more symbols that contain the same key, and further obtain the key with a higher probability. In short, the KS can be enhanced by moving the key bit to a lower ρ and/or decreasing λ.

KDR can be obtained as $KDR = Baud\ rate / \lambda$, which is inversely proportional to λ. On the other hand, KER can be reduced by increasing λ according to our previous work [23]. There is a trade-off among KS, KER, and KDR, depending on ρ and λ, which is summarized in Table I. The desired result is a system that achieves higher KS, lower KER, and higher KDR.

Therefore, we propose a parameter self-adaptive strategy to adjust ρ and λ to the optimal comprehensive performance among KER, KDR, and KS.

It should be noted that this strategy can be simplified by setting constant KER. Since the distributed key can be only used for encryption and decryption when the error-free key is

TABLE I
IMPACT ON PERFORMANCE INDICATORS

	KS	KER	KDR
Lower ρ	↑	---	---
Increasing λ	↓	↓	↓

This article has been accepted for publication in IEEE/OSA Journal of Lightwave Technology. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/JLT.2023.3257963

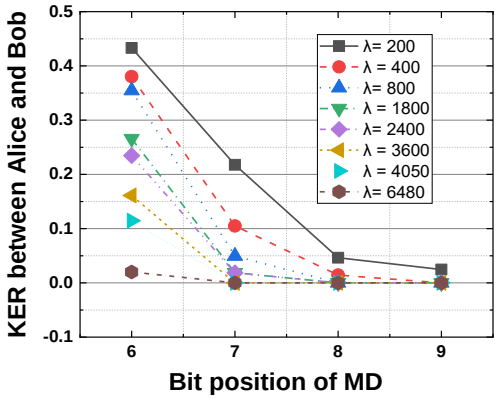

Fig. 6. KER between Alice and Bob as a function of bit position of MD.

shared between two legitimate parties. Given such a KER threshold, the proposed strategy aims to obtain the minimum λ under the lowest ρ.

Fig. 5 presents the flow chart of the parameter self-adaptive strategy. The operation steps are described as follows:

(1) Initialization. The mapped data of I/Q are N bits per symbol. Therefore, the set of MD's bit position is $\rho = \{\rho_i, \rho_{i+1}, \ldots \rho_N\}$ where $i \in \{2,3,...,N-2\}$. ρ_1 is not being counted in since it is the first basis state and needs to operate XOR operation with MD. The set of bit duplication times is $\lambda = \{\lambda_j, \lambda_{j+1}, \ldots \lambda_M\}$ where $j \in \{1,2,...,M-2\}$.

(2) KER comparison. Set $\rho = \rho_i$, $\lambda = \lambda_j$ where $i = 2$, $j = 1$. Then the key is distributed. If the KER is not higher than the threshold of preset KER, the optimal ρ is ρ_2, and optimal λ is λ_1. Otherwise, keep sweeping ρ_i and λ_j until the threshold of preset KER is reached. It should be illustrated that the KER threshold can be set in ranges from 0 to 10%. It is because the error-free key can be obtained through information reconciliation when the KER is less than 10% [24].

(3) Updating the optimal ρ_i and λ_j.

We implement the proposed parameter self-adaptive strategy in our experimental system (part A of section II) over 300km ultra-low loss fiber (ULF). The KER threshold is preset as zero. $\rho = \{6,7,8,9\}$, $\lambda = \{200,400,800,1800,2400,3600,4050,6480\}$ .As shown in Fig.6, the KER is illustrated as a function of the bit position of MD ρ and λ. The optimal ρ is 7 and the optimal λ is 3600. α is equal to zero. It is worth noting that setting $\alpha = 0$ in the case of $\lambda \geq 3600$ can directly obtain an error-free key, which can reduce the key distribution time by omitting the execution of information reconciliation (IR). The corresponding KDR is 277K bits/s. In addition, the results show that the higher ρ, the lower KER can be obtained under the same KDR.

III. Security Analysis and Improvement

The security analysis is conducted based on three assumptions: (1) Eavesdropper, namely Eve, does not have access to the legitimate users' local offices; (2) Eve has the same devices as legitimate parties for signal capture and can obtain a half amount of signal power (~50%); and (3) Eve knows the system parameters, such as ρ and λ, as the same as the legitimate parties. We analyze the security of the proposed system under a typical fiber-tapping attack and evaluate the difficulty for Eve to recover the key. The following analysis uses the same experimental platform and setup as in Part B of Section II.

- We evaluate the eavesdropper's performance of direct detection and demodulation of the MD that carried the key.
- We increase Eve's eavesdropping abilities by reducing the basis state difference between the legitimate part and Eve and reconstructing the key recovery.
- We introduce privacy amplification for the leaked raw key to obtain the ultimately secure key.

A. *Key eavesdropping via tapping attack*

The ability of the eavesdropper to recover the key by using direct tapping at the uplink and downlink is analyzed firstly. Before recovering the key, Eve should detect and demodulate the signal. On the detection side, Eve directly captures signals from uplink and downlink respectively. Then, Eve demaps her detected symbols using the same method as the asymmetric basis state Y-00 protocol. The basis state of Eve is independent of the legitimate parties. Since the proposed scheme utilizes the same physical effects (e.g., quantum noise and ASE noise) and XOR operation as the Y-00 protocol in principle, the received signal noise distribution is also used to evaluate the demodulation performance of Eve. Moreover, the number of noise masks [25], named Γ, is calculated as the indicator of the security of the tapped signals, which can be obtained as

$$\Gamma = \Gamma_I \times \Gamma_Q = \left(\frac{2\bar{\sigma}_I}{\Delta}\right) \times \left(\frac{2\bar{\sigma}_Q}{\Delta}\right) \tag{2}$$

where $\Delta = 2/(M-1)$, M is the order of the mapped signal in both I and Q data. The noise variances of MD carried by I and Q channel are $2\bar{\sigma}_I$ and $2\bar{\sigma}_Q$,

$$\bar{\sigma}_I = \sqrt{\frac{1}{2}\sum_{n=1}^{2}\sigma_{I,n}^2} \qquad \bar{\sigma}_Q = \sqrt{\frac{1}{2}\sum_{n=1}^{2}\sigma_{Q,n}^2} \tag{3}$$

The calculation results show that Γ are 25426 and 113370 for $2^{10}\times2^{10}$ QAM in uplink and downlink respectively. It is practically difficult to directly demodulate the MD that carried the key from both uplink and downlink.

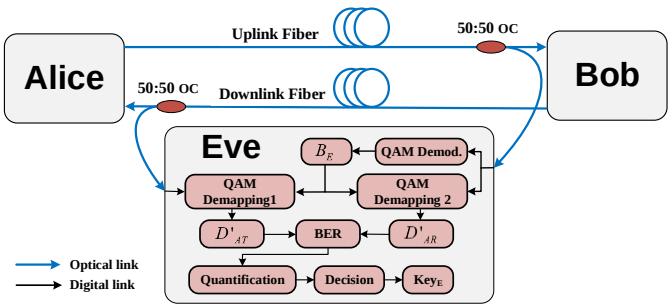

Fig. 7. The signal tapping attack for reduction of the basis state difference and key recovery.

This article has been accepted for publication in IEEE/OSA Journal of Lightwave Technology. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/JLT.2023.3257963

B. *Reduction of the Basis State Difference and Key Recovery*

An attack method is illustrated in Fig. 7. Eve eavesdrops on the signal on Bob's side when Alice sends a signal to the other part. According to Fig. 1, the security of the proposed key distribution comes from the basis state difference between Alice and Eve. Eve must reduce the basis state difference before she can correctly recover the key. In other words, Eve needs to perform a series of operations to obtain the same basis as Alice. In our analysis, Eve uses the demodulated QAM signal B_E obtained by attacking the uplink as the basis states for both the uplink and downlink. The reason is that the basis state of the higher bit position of the symbols has a lower bit error rate in propagation [21]. These basis states are rarely masked by noise and exposed or partially exposed to Eve.

As shown in Fig. 7, in a tapping attack Eve uses a 50:50 optical coupler (OC) to tap the signal from fibers. Eve demodulates the $2^{10}\times2^{10}$ QAM/DFTs-OFDM mapped symbols and obtains 10 bits sequences per symbol in the I/Q channel, namely Eve's basis state B_E. Then, Eve utilizes B_E to demap the detected symbols using the same method as the asymmetric basis state Y-00 protocol. Finally, Eve obtains her key by measuring and analyzing the BER curves using (1). The experiment results show that KER between Eve and legitimate parties is 0.25 with λ of 3600. The mutual information between the legitimate and the illegitimate part is 1.836×10^{-1}, which means that there is partly raw key information leakage.

C. *Privacy Information*

In tapping-based eavesdropping, Alice and Bob share a sequence of bits, i.e., the raw key while the eavesdropper may obtain partial information. The approach to transforming this partially secure raw key into an ultimately secure key is called privacy amplification, which was firstly described in the context of quantum key distribution protocols in [26-28]. In our system, a secure hash algorithm, SHA3-512, is used to perform privacy amplification that converts a partially secure key into the ultimately secure key. After the privacy information, the mutual information between legitimate and illegitimate part decrease from 1.836×10^{-1} to 3.0875×10^{-5}, indicating improved security of the key sequences is obtained by privacy amplification. The final KDR is 39.3 (277×512/3600) Kbits/s.

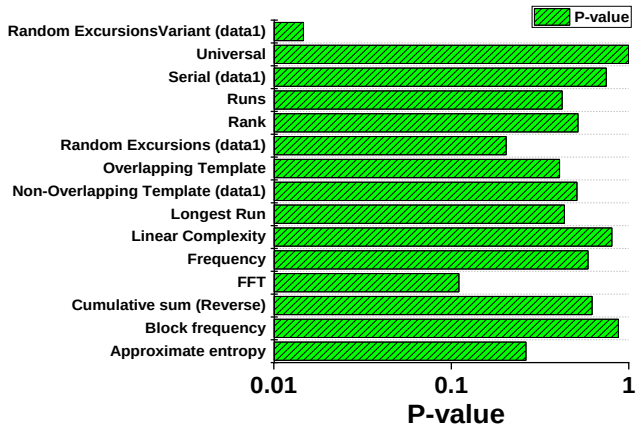

Fig. 8. NIST randomness test results.

D. *Randomness Test*

Key randomness is an important indicator to be tested before an encryption application. To evaluate the randomness of the obtained virtual secret key, the national institute of standards and technology (NIST) test suite is employed. All of the 15 indexes are evaluated using a key sequence with a length of 10^6. If the P-value > 0.01 can be achieved in each index of the NIST test, the randomness of the sequences can be ensured. Fig. 8 shows the results of the test, which confirms the randomness of the distributed key in the proposed scheme.

IV. Integration of QNSC and Key Distribution

We experimentally combine QNSC with the proposed key distribution and analyze the Q factor penalty in the integrated PLSOC system. To simplify the demonstration, we use the symbol bit position diagram of the In-phase channel to illustrate the integration of QNSC and the proposed key distribution in Fig. 9. The quadrature channel has the same bit position diagram as the In-phase channel. In the In-phase channel, D_I is the plaintext data before encryption or mapping, R_I is the 1st basis state, B_I is the other basis states, and S_I is the MD.

The non-overlapping available bit position, namely non-overlapping available bandwidth resources, for key distribution and encryption provides the potential for the integration of QNSC and key distribution. In Fig. 9(a), the 7th bit of a symbol transmits MD for key distribution. As shown in Fig. 9(b), the highest bit of a symbol is used to transmit the encrypted plaintext data in the QNSC system. The integration of QNSC and the key distribution can be achieved by allocating the plaintext data bit and the key bit in one symbol as shown in Fig. 9(c). Specifically, we can perform QNSC in the 10th bit of a symbol and distribute the key using the 7th bit simultaneously except for the first-time key distribution. Since the proposed key distribution does not share the same seed key, the first-time key distribution cannot be integrated with QNSC.

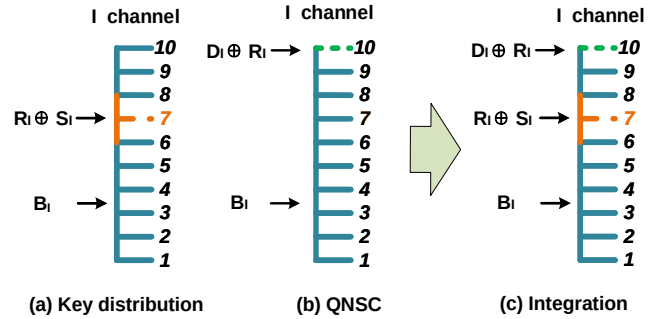

Fig. 9. The bit position diagram in In-phase channel of per symbol for integration of QNSC and key distribution.

To validate the integrated system, as shown in Fig. 10, the experimental platform and setup are the same as the one in Part B of Section II over 300km ULF. The ρ is optimal value 7. and λ is set as 3600. Among the key post-processing module include information reconciliation and privacy amplification. A gray image of the experiment platform is transmitted and received for evaluation of the proposed PLSOC system. The bit rate of the QAM/QNSC is 10Gbps (10Gbaud ×2bit/symbol×

This article has been accepted for publication in IEEE/OSA Journal of Lightwave Technology. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/JLT.2023.3257963

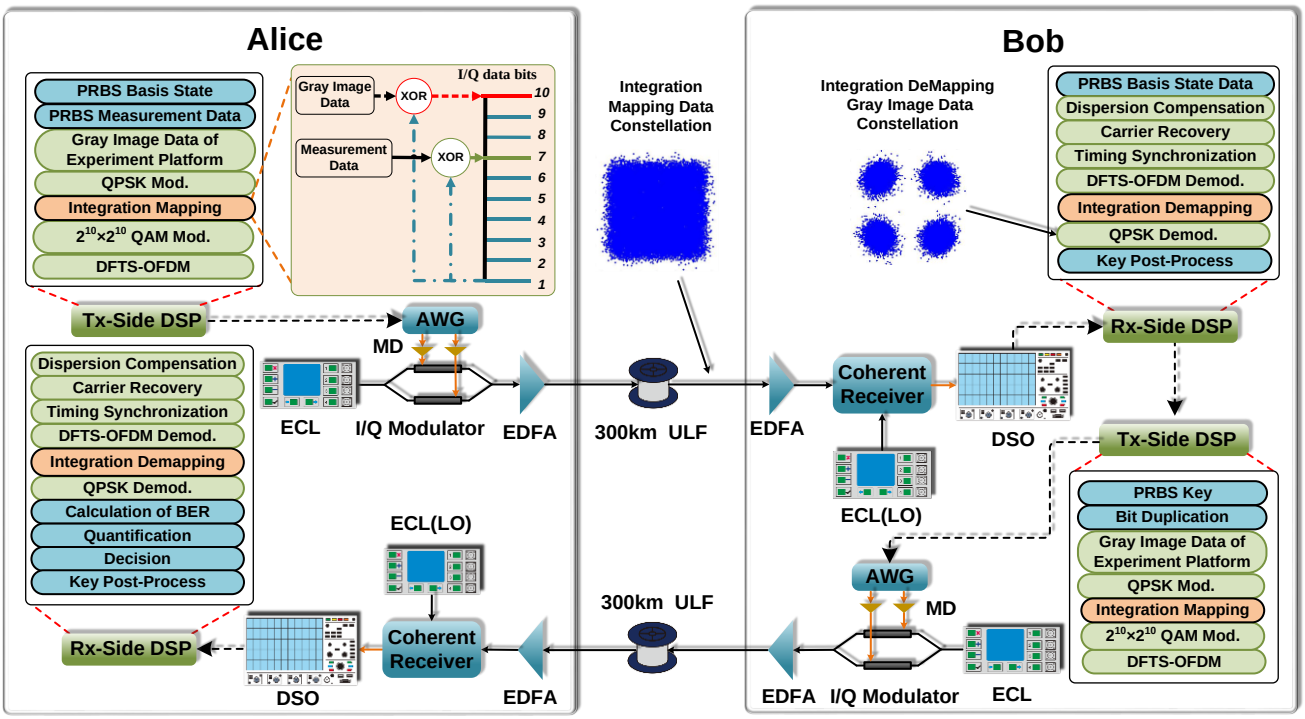

Fig. 10. Integration of key distribution and QNSC experiment over 300km ULF. ECL: External Cavity Laser; MD: Modulator Driver; AWG: Arbitrary Waveform Generator; EDFA: Erbium-Doped Fiber Amplifier; LO: Local-oscillator; DSO: Digital Storage Oscilloscope; DFTs-OFDM: Discrete Fourier Transform Spread Orthogonal Frequency Division Multiplexing.

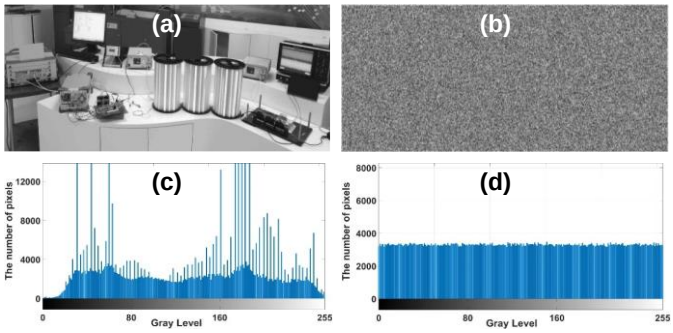

Fig. 11. (a) Gray image of experiment platform demodulated by legitimate part; (b) Gray image of experiment platform eavesdropped by Eve; (c) Gray image histogram of experiment platform demodulated by legitimate part; (d) Gray image histogram of experiment platform eavesdropped by Eve.

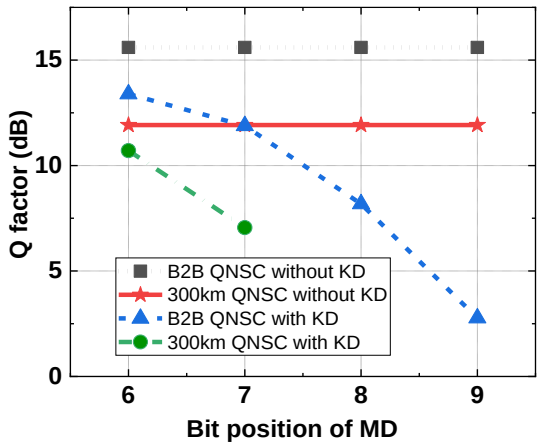

Fig. 12. The Q factor of system where QNSC with and without integration key distribution. B2B: Optical Back-to-Back, KD: Key Distribution.

1/2), where the AWG sampling rate is 10GSa/s, the modulation format is QPSK, and the bandwidth utilization rate is 1/2 due to the DFTS-OFDM. The gray image of the experiment platform recovered by the legitimate part and eavesdropper are shown in Fig. 11(a) and (b) respectively. The legitimate parties can correctly demodulate the original plaintext data. However, the eavesdropper cannot obtain the original plaintext data. Furthermore, as illustrated in Fig. 11(c) and (d), the pixel numbers of the gray levels are shown. Compared with one of the legitimate parties, an almost uniform distribution of the gray levels can be found by the eavesdropper. The results verify the feasibility of the integration of QNSC and the key distribution

In addition, we evaluate the transmission performance penalty of the integrated system. In Fig. 12, the Q factor of the plaintext data encrypted by QNSC decreases as the bit position of MD ρ increases. It can be attributed to the fact that the MD carried key is equal to noise data in the QNSC aspect. Because the MD is irrelevant to the basis state and changes with the distributed key. From the knowledge of digital-to-analog conversion, we know that the ρ increases by one bit, the size of the introduced noise ground doubles. Finally, in our experimental platform, the Q factor penalty of the system is 3.7dB (optical back-to-back) and 4.8dB (300km) where the ρ is 7.

V. Conclusion

In this paper, a compatible physical-layer secure optical communication (PLSOC) system that integrates self-adaptive physical-layer key distribution and encryption in optical coherent communication is proposed and experimentally demonstrated. We propose a key distribution scheme based on

the BER difference of QAM signals mapped by asymmetric basis state Y-00 protocol. KS, KER, and KDR of the system are discussed as the key performance metrics of the system, which are the joint results of the system parameters including MD's bit position ρ, and the bit duplication times λ. An adaptive strategy is proposed for ρ, λ and privacy amplification is used for the improvement of security. The proposed physical-layer key distribution is realized by only DSP, indicating good compatibility with the high-speed transmission system as well as the integrability with the encryption. The experiment is carried out to validate the proposed scheme. A key distribution distance of 300km is successfully demonstrated when the optimal λ and ρ. The KDR is 39.3Kbits/s with zero KER. The security is improved by privacy amplification using SHA3-512. the mutual information between legitimate and illegitimate parts decreased from 1.836×10^{-1} to 3.0875×10^{-5}, which indicates the improved security of the key. Moreover, we experimentally demonstrate the integration of QNSC and the key distribution system. The transmission performance penalty of the integrating system is also evaluated, 3.7dB (optical back-to-back) and 4.8dB (300km) Q factor penalties are achieved, respectively. Since the proposed PLSOC system is achieved by digital signal processing only, it is highly compatible with the current optical transmission system without the demand to change the structure of the optical communication node.

REFERENCES

[1] G. N. Skorin-Kapov, M. Furdek, S. Zsigmond, and L. Wosinska, "Physical-layer security in evolving optical networks," *IEEE Commun. Mag*., vol. 54, no. 8, pp. 110-117, Aug. 2016.

[2] G. S. Kanter, D. Reilly and N. Smith, "Practical physical-layer encryption: The marriage of optical noise with traditional cryptography," *IEEE Commun. Mag*., vol. 47, no. 11, pp. 74-81, Nov. 2009.

[3] M. Yoshida, T. Hirooka, K. Kasai, and M. Nakazawa, "Single-channel 40 Gbit/s digital coherent QAM quantum noise stream cipher transmission over 480 km," *Opt. Exp*., vol. 24, no.1, pp. 652-661, Jan. 2016.

[4] M. Yoshida, T. Kan, K. Kasai, T. Hirooka, and M. Nakazawa, "10 Tbit/s QAM quantum noise stream cipher coherent transmission over 160 Km," *J. Lightw. Technol*., vol. 39, no. 4, pp. 1056-1063, May. 2021.

[5] M. Nakazawa, M. Yoshida, T. Hirooka, K. Kasai, T. Hirano, T. Ichikawa, and R. Namiki, "QAM quantum noise stream cipher transmission over 100 km with continuous variable quantum key distribution," *IEEE J. Quantum Electron*., vol. 53, no. 4, pp.1-16, May. 2017.

[6] J. Katz and Y. Lindell, Introduction to Modern Cryptography. Boca Raton, FL, USA: Chapman & Hall, 2007.

[7] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," *Rev. Mod. Phys*., vol. 74, no. 1, pp. 145-195, Mar. 2002.

[8] A. Argyris, E. Pikasis, and D. Syvridis, "Gb/s one-time-pad data encryption with synchronized chaos-based true random bit generators," *J. Lightwave Technol*., vol. 34, no. 22, pp. 5325-5331, Oct. 2016.

[9] N. Li, H. Susanto, B. Cemlyn, I. D. Henning, and M. J. Adams, "Secure communication systems based on chaos in optically pumped spin-VCSELs," *Opt. Lett*., vol. 42, no. 17, pp. 3494-3497, Sep. 2017.

[10] N. Jiang, A. Zhao, C. Xue, J. Tang, and K. Qiu, "Physical secure optical communication based on private chaotic spectral phase encryption/decryption," *Opt. Lett*., vol. 44, no. 7, pp. 1536-1539, Mar. 2019.

[11] W. Shao, M. Cheng, L. Deng, Q. Yang, X. Dai, and D. Liu, "High-speed secure key distribution using local polarization modulation driven by optical chaos in reciprocal fiber channel," *Opt. Lett*., vol. 46, no. 23, pp. 5910-5913, Nov. 2021.

[12] A. A. E. Hajomer, L. Zhang, X. Yang, and W. Hu, "284.8-Mb/s physical-layer cryptographic key generation and distribution in fiber networks," *J. Lightwave Technol*., vol. 39, no. 6, pp. 1595-1601, Dec. 2021.

[13] L. Zhang, A. A. E. Hajomer, W. Hu, and X. Yang, "2.7 Gb/s secure key generation and distribution using bidirectional polarization scrambler in fiber," *IEEE Photonics Technol. Lett*., vol. 33, no. 6, pp. 289-292, Feb. 2021.

[14] L. Zhang, X. Huang, W. Hu, and X. Yang, "Point to multi-point physical-layer key generation and distribution in passive optical networks," *Opt. Lett.*, vol. 46, no. 13, pp. 3223-3226, Jun. 2021.

[15] X. Wang, J. Zhang, Y. Li, Y. Zhao, and X. Yang, "Secure Key Distribution System Based on Optical Channel Physical Features," *IEEE Photon. J*., vol. 11, no. 6, pp. 1-11, Nov. 2019.

[16] X. Wang, Y. Li, Y. Zhao, C. Lei, H. Zhang, and J. Zhang, "Physical layer authentication based on BER measurement of optical fiber channel," *IEEE Access*, vol. 8, pp. 101812–101823, May. 2020.

[17] K. Zhu, J. Zhang, Y. Li, W. Wang, X. Liu, and Y. Zhao, "Experimental demonstration of error-free key distribution without an external random source or device over a 300-km optical fiber," *Opt. Lett*., vol. 47, no. 10, pp. 2570-2573, May. 2022.

[18] M. Dong, J. Zhang, H. Zhang, Y. Zhao, Y. Li, and C. Lei, "Key Distribution Scheme Based on Uneven PSK Modulation Using Phase Noise," in *Proc. Opto-Electron. Commun. Conf*., Taipei, Taiwan, 2020, pp.1-3.

[19] S. We, Y. Li, K. Zhu, C. Lei, Y. Zhao, and J. Zhang, "Physical-layer Secure Key Distribution Scheme Based on Phase Noise in PSK/QNSC," in *Proc. Asia Commun. Photon. Conf.*, Shanghai, China, 2021, pp. W3B-7.

[20] C. Lei, J. Zhang, Y. Li, Y. Zhao, H. Yu, and Y. Zhang, "Key Distribution Based on Survival Life Time with Y-00 Protocol in Optical Fiber Link," in *Proc. Opto-Electron. Commun. Conf*., Fukuoka, Japan, 2019, pp1-3.

[21] 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, Feb. 2014.

[22] J. Li, Y. Li, B. Wang, K. Wang, Y. Zhao, and J. Zhang, "Ciphertext Mapping Method based on Gray Code in Quantum Noise Stream Cipher," in *Proc. Int. Conf. Opt. Commun. Netw*., Qufu, China, 2021, pp. 1-3.

[23] C. Lei, J. Zhang, Y. Li, Y. Zhao, B. Wang, H. Gao, J. Li, and M. Zhang, "Long-Haul and High-Speed Key Distribution Based on One-Way Non-Dual Arbitrary Basis Transformation in Optical Fiber Link," in *Proc. Opt. Fiber Commun. Conf*., San Diego, CA, USA, 2020, pp.1-3.

[24] Z. Tu, J. Zhang, Y. Li, Y. Zhao, C. Lei, X. Yang, and Y. Sun, "Experiment Demonstration of Physical Layer Secret Key Distribution with Information Reconciliation in Digital Coherent Optical OFDM System," in *Proc. Asia Commun. Photo. Conf*., Chengdu, China, 2019, pp.1-3.

[25] C. Lei, J. Zhang, Y. Li, Y. Zhao, K. Wang, S. Liu, and J. Li, "16 QAM Quantum Noise Stream Cipher Coherent Transmission Over 300 km Without Intermediate Amplifier," *IEEE Photonics Technol. Lett*., vol. 33, no. 18, pp. 1002-1005, May. 2021.

[26] C. H. Bennett, G. Brassard, and J.-M. Robert, "Privacy amplification by public discussion," *SIAM J. Comput*., vol. 17, no. 2, pp. 210–229, Apr. 1988.

[27] C. H. Bennett, G. Brassard, C. Crépeau, and U. M. Maurer, "Generalized privacy amplification," *IEEE Trans. Inf. Theory*, vol. 41, no. 6, pp. 1915–1923, Nov. 1995.

[28] U. Maurer and S.Wolf, "Secret-key agreement over unauthenticated public channels-Part III: Privacy amplification," *IEEE Trans. Inf. Theory*, vol. 49, no. 4, pp. 839–851, Apr. 2003.