Probabilistic Shaping-Assisted Bases Precoding in QAM Quantum Noise Stream Cipher

photonics

MDPI

Article

Probabilistic Shaping-Assisted Bases Precoding in QAM Quantum Noise Stream Cipher

Shuang Wei [1,†], Sheng Liu [2,†], Wei Wang [1], Chao Lei [3], Kongni Zhu [4], Mingrui Zhang [1], Yuang Li [1], Yunbo Li [2], Dong Wang [2], Dechao Zhang [2], Han Li [2], Yajie Li [1,*], Yongli Zhao [1] and Jie Zhang [1,*]

[1] State Key Laboratory of Information Photonic and Optical Communication, Beijing University of Posts and Telecommunications, Beijing 100876, China; ws28@bupt.edu.cn (S.W.); weiw@bupt.edu.cn (W.W.); mingruizhang@bupt.edu.cn (M.Z.); lya2020@bupt.edu.cn (Y.L.); yonglizhao@bupt.edu.cn (Y.Z.)
[2] Department of Fundamental Network Technology, China Mobile Research Institute, Beijing 100053, China; liushengwl@chinamobile.com (S.L.); liyunbo@chinamobile.com (Y.L.); wangdongyjy@chinamobile.com (D.W.); zhangdechao@chinamobile.com (D.Z.); lihan@chinamobile.com (H.L.)
[3] Electrical Engineering Department, Chalmers University of Technology, 41296 Gothenburg, Sweden; chaole@chalmers.se
[4] School of Computer Science and Engineering, Xi'an University of Technology, Xi'an 710048, China; zhukongni@xaut.edu.cn
* Correspondence: yajieli@bupt.edu.cn (Y.L.); jie.zhang@bupt.edu.cn (J.Z.); Tel.: +86-132-6948-6368 (Y.L.)
† These authors contributed equally to this work.

Abstract

We propose a probabilistic shaping-assisted base precoding quantum noise stream cipher (PSABP QNSC) scheme to effectively alleviate the encryption penalty in QAM QNSC systems. In contrast to the uniformly distributed bases adopted in traditional QNSC, Gaussian distributed bases can provide shaping gain. We theoretically analyze the underlying gain mechanism of Gaussian distributed bases in the PSABP QNSC scheme. Experimental results of 160 km reveal that the encryption penalties of QPSK and 16QAM are reduced by 0.44 dB and 0.27 dB, in terms of OSNR. Moreover, the security is quantified through the number of masked signals as a primary key metric. To mitigate the impact of base precoding, we propose the effective bases and effective ciphertext symbol points to refine the security evaluation. Moreover, the security is estimated in terms of mutual information leakage, with 2.2×10^{-4} bits of QPSK and 1.85×10^{-4} bits of 16QAM. The results indicate that the PSABP QNSC scheme provides effective protection against eavesdropping.

Keywords: quantum noise stream cipher; probabilistic shaping; quadrature amplitude modulation

Received: 9 February 2026
Revised: 18 March 2026
Accepted: 18 March 2026
Published: 23 March 2026

1. Introduction

Optical fiber communications have been widely deployed in commercial core and metro communication networks, benefiting from their strong stability, high capacity, and long-haul transmission [1]. However, driven by illegal interests, personal privacy and confidential information face tremendous security risks, hence security has been a non-neglected property in communication systems. Compared with traditional mathematical encryption algorithms, physical-layer secure encryption schemes have the unique advantage of resisting the attack of quantum computers [2]. To improve the security of communication systems, physical-layer secure encryption schemes have attracted extensive attention [3,4].

Based on the Born rule principle, quantum noise from equipment in the optical communication system is unable to be eliminated in any way [5]. The minimum Euclidean distance is an effective criterion for evaluating the bit error ratio (BER) performance [6]. When the Euclidean distance between adjacent symbols in the constellation is small enough, they are confused by noise so much that they are incapable of being distinguished accurately. Therefore, the theoretical optimal BER performance is affected by quantum noise. Quantum noise stream cipher (QNSC) is a physical-layer secure encryption scheme taking advantage of unescapable quantum noise (e.g., shot noise) [7]. In the QNSC system, the plaintext symbols, with low-order modulation format, are randomly mapped into the ciphertext symbols with ultra-high-order modulation format, so-called QNSC symbols. Due to the quantum noise masking effect, a QNSC symbol becomes indistinguishable from its surrounding QNSC symbols. The QNSC symbols can be transformed into low-order symbols in the same way as the plaintext symbols by legal parties with pre-shared secret keys, while the attacker (Eve) only demodulates the ultra-high-order QNSC symbols. This feature ensures that the QNSC system can resist eavesdropping attacks and protect the security of personal privacy and confidential information.

Recently, the major research purpose has focused on two aspects: security enhancement and transmission performance improvement. In terms of security enhancement, the security of QNSC is further discussed under correlation, known-plaintext, and quantization attacks [8–10]. The masking effects of shot noise and amplified spontaneous emission (ASE) noise are theoretically analyzed under various average optical power and optical signal-to-noise ratio (OSNR) [11]. A novel optical stealth communication scheme based on the ASE light source is proposed to improve the number of masked signals (NMS) [12]. Based on randomized perturbation, an excellent NMS is guaranteed at the cost of transmission performance [13]. The hyperchaotic system provides extra diffusion for security enhancement in QAM/QNSC [14]. It is possible to achieve the integration of secure transmission and key distribution with the multi-bit mapping Y-00 protocol [15]. In terms of improving transmission performance, an attractive work reaches ultra-long-haul digital coherent PSK/QNSC with 10,118 km fiber transmission [16]. A 300 km fiber transmission without an intermediate amplifier is achieved, benefiting from the subtractive clustering method and optimized fuzzy C-means clustering algorithm in [17]. A low encryption penalty LEO-to-Earth Secure Laser Communication Based on Quantum Noise Stream Cipher is proposed [18]. Using end-to-end deep learning, a 400 Gbps QNSC is implemented over 1520 km fiber in a 21-channel WDM transmission system [19]. The single-channel net rate in QAM/QNSC was higher than 200 Gbps in [20,21]. However, there is a trade-off between transmission performance and security, and that is, high security often sacrifices transmission performance as a cost. The encryption penalty in QAM/QNSC is demonstrated due to adding bases and expanding constellation space [21].

Probabilistic shaping (PS) is an effective technique to approach the Shannon limit by adjusting the occurrence frequency of symbols [22–24]. By optimizing the symbol distribution, the PS signal can achieve better BER performance than a uniformly distributed signal at the same OSNR. In previous work [20], PS is applied to the payload constellation of 16QAM, while uniform bases are still used to construct QNSC symbols. However, since the encryption penalty in QNSC is inherently induced by adding bases, optimizing only the payload distribution cannot fundamentally mitigate the encryption penalty. Since the encryption penalty decreases with the increase in the plaintext modulation order [21], 256QAM encryption can be achieved without the encryption penalty utilizing a delta sigma modulator [25–27]. However, relatively low-order plaintext modulation formations still dominate practical applications. Therefore, it is worth studying new approaches to improve

transmission performance and mitigate encryption penalty for relatively low plaintext modulation orders.

In previous work, we have proposed a PS-assisted base precoding QNSC (PSABP QNSC) scheme and utilized non-uniform bases to effectively mitigate encryption penalties [28]. In this paper, we further extend previous work from the following aspects:

(i) Theory: We theoretically analyze the gain mechanism with Gaussian bases and explore the effect of various shaping rate parameters λ on the minimum Euclidean distance in the QAM/QNSC system. PS gains are systematically evaluated across QNSC ciphertext constellations, with comparative analysis of QPSK and 16QAM plaintext symbol configurations. Compared with the traditional QNSC signal, our proposed scheme realizes an achievement in alleviating the encryption penalty and improving BER performance.

(ii) Experiment: We set up an experimental platform of a coherent optical transmission system and measure the BER performance curves of 160 km standard single-mode fiber (SSMF). The shaping rate parameter λ and block length L are set to satisfy the code rate of $(m-1)/m$, which m is the total number of bits of a basis for the I or Q component. Experimental results demonstrate that the proposed PSABP QNSC schemes achieve encryption penalties of 0.16 dB and 0.14 dB for QPSK and 16QAM, respectively, corresponding to reductions of 0.44 dB and 0.27 dB, at the 15% overhead soft-decision forward error correction (SD-FEC) threshold over a 160 km SSMF transmission link. The comparison between this scheme and other schemes is shown in Table 1.

(iii) Security: We investigate the effect of Gaussian distributed bases on the security of QNSC. The effective bases and effective ciphertext symbol points are proposed to optimize the calculation expression of NMS. The NMS and detection failure probability (DFP) are discussed at the eavesdropping point. Furthermore, we evaluate the mutual information of Eve in terms of quantum noise and all noise. The mutual information leakage is 2.2×10^{-4} bits for QPSK, compared to 1.85×10^{-4} bits for 16QAM. The results demonstrate that the PSABP QNSC scheme can effectively resist eavesdropping by Eve.

Table 1. The comparison of QAM/QNSC.

Ref.	Distance (km)	Data Rate (Gbps)	Plaintext	QNSC	Encryption Penalty	Mutual Information Leakage (bit)
[14]	30	50 *	16QAM	2^{16}	No analysis	2.29×10^{-4}
[15]	45	20 *	QPSK	2^{20}	No analysis	-
[17]	300	40 *	16QAM	2^{16}	No analysis	1.58×10^{-4}
[20]	1200	201.6 **	16QAM	2^{16}	No analysis	7.08×10^{-4}
[21]	640	205.9 **	16QAM	2^{16}	OSNR 0.67 dB	2.7×10^{-3}
[26]	400	163 **	256QAM	2^{40}	No penalty	4.05×10^{-10}
Our	160	14 **	16QAM	2^{20}	OSNR 0.14 dB	1.85×10^{-4}
	160	7 **	QPSK	2^{20}	OSNR 0.16 dB	2.2×10^{-4}

* Line rate; ** Net rate.

2. Principle of PSABP QNSC

This section introduces the CCDM algorithm briefly, the principle of the QNSC system and the design of the PSABP QNSC scheme.

2.1. CCDM Algorithm

The key idea of the PS algorithm is to modify the symbol probability distribution so that the transmitted signal is better matched to the channel. In an additive white Gaussian noise (AWGN) channel, signals following a Gaussian distribution generally achieve superior transmission performance. To match the Gaussian distribution, Maxwell–Boltzmann (MB) distribution usually is employed, which is one of Gaussian-like distributions. In a given M-PAM symbols set $\mathcal{X} = \pm 1, \pm 3, \ldots, \pm(M-1)$, $\boldsymbol{x}$ represents the symbol in set $\mathcal{X}$. The expression of the MB distribution can be expressed by $\boldsymbol{x}$ as follows:

$$P(\boldsymbol{x}) = \frac{e^{-\lambda \boldsymbol{x}^2}}{\sum_{\boldsymbol{x}' \in \chi} e^{-\lambda \boldsymbol{x}'^2}} \tag{1}$$

where λ, with a non-negative number, is the shaping rate parameter. As λ increases, lower amplitude symbols occur with higher probability, while higher amplitude symbols occur with lower probability.

The probabilistic amplitude shaping architecture with CCDM is a common method used for PS [29,30]. The function of CCDM is to encode the input uniform bit sequences into a positive decimal number with desired probability, as shown in Figure 1. There is an assumption that the number of input bits is α, the number of output bits is β. Then, the code rate is α/β. The block length L determines the number of output symbols of CCDM.

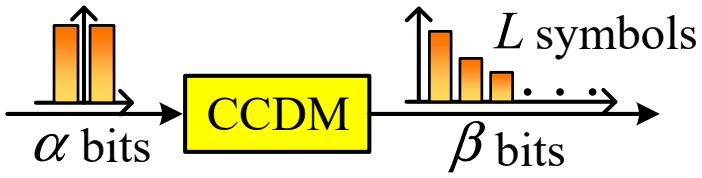

Figure 1. The schematic of CCDM.

2.2. The Principle of QNSC

QNSC adopts the expansion of the constellation space to enhance system security. First, XOR operation in which the plaintext bit is XORed with the least significant bit of the basis, where the resulting bit sequence is denoted by R_a, and the basis bit sequence is denoted by R_b. Second, expansion operation in which R_a and R_b are treated as the higher-bit part and lower-bit part, respectively, to form a new bit sequence R_c. For clarity, let $\boldsymbol{a}$, $\boldsymbol{b}$, and $\boldsymbol{c}$ denote the corresponding decimal domain symbols mapped from R_a, R_b, and R_c, respectively. In the QAM/QNSC system, the expansion constellation space principle can be expressed as follows:

$$\boldsymbol{c} = f(\boldsymbol{a}) + g(\boldsymbol{b}), \tag{2}$$

$$f(\boldsymbol{x}) = \boldsymbol{x} \bullet 2^m, \tag{3}$$

$$g(\boldsymbol{x}) = 2\boldsymbol{x} + (-2^m + 1, -2^m + 1) \tag{4}$$

where m represents the total bit number of a basis bit sequence. For example, let the plaintext bit sequence be $(10, 00)$, and let the basis bit sequence be $R_b = (0110, 1011)$. After the XOR operation, the resulting bit sequence is $R_a = (10, 11)$. In the expansion step, R_a and R_b are treated as the higher-bit part and lower-bit part, respectively, yielding $R_c = (011010, 101111)$, where the bit significance increases from left to right. In the decimal domain, the plaintext symbol corresponding to $(10, 00)$ is $(-1, -3)$, $R_b = (0110, 1011)$, which corresponds to $\boldsymbol{b} = (6, 13)$, and $R_a = (10, 11)$ corresponds to $\boldsymbol{a} = (-1, 3)$. According to Equations (2)–(4), $\boldsymbol{c} = f(\boldsymbol{a}) + g(\boldsymbol{b}) = f(-1, 3) + g(6, 13) = \left(-1 \times 2^4 + 2 \times 6 - 2^4 + 1, 3 \times 2^4 + 2 \times 13 - 2^4 + 1\right) = (-19, 59)$. Therefore, 16QAM is encrypted into 64 × 64QAM using 16 × 16QAM bases.

Increasing m reduces the Euclidean distance between adjacent symbols in the QNSC constellation, making reliable symbol discrimination increasingly difficult in the presence of noise masking. The legal parties with shared secret keys have the capability to convert QNSC symbols to lower-order symbols, reducing the impact of noise masking. However, the illegal parties without shared secret keys only demodulate high-order QNSC symbols with noise masking. In a QNSC symbol, the BER varies across different bit positions [8]. Bits in the more significant positions are more likely to be recovered by Eve, whereas those in the less significant positions remain better protected. The larger the m, the more seriously the bits in lower positions are obscured by noise. Therefore, Eve hardly recovers the plaintext bit from the intercepted symbol $\boldsymbol{a}$.

2.3. The Design of PSABP QNSC Scheme

Figure 2 shows the schematic diagram of the principle of the PSABP 16-QAM/QNSC scheme. The seed key1 and key2 are pre-shared between legal parties, namely Alice and Bob. The two pseudorandom number generators (PRNG1 and PRNG2) are adopted to generate running keys with seed keys. One of them encrypts the plaintext bit by bit, the first step of encryption. The other is regarded as the original bases to expand constellation space, the second step of encryption. For the I or Q component, each two bits are modulated to 4PAM symbol A_I and A_Q adopting gray mapping. A_I and A_Q are translated into high-order symbol $A_I{}'$ and $A_Q{}'$. The shaping rate parameter λ and block length L are used to initialize CCDM modules. The code rate $m-1/m$ is set by adjusting λ and L. In effect, the code rate being set to other values also applies to PSABP QNSC. The original bases are input into the PS modules to generate encoded bases with MB distribution. The total bit number of encoded bases increases due to redundancy brought by PS. Note that an original basis is composed of $m-1$ bits, while an encoded basis is composed of m bits. Similarly, the encoded bases B_I and B_Q are also mapped into high-order B_I' and B_Q'. The symbols of I and Q components are obtained by $A_I{}' + B_I'$ and $A_Q{}' + B_Q'$, where the amplitudes range from $-2^{2+m}+1$ to $2^{2+m}-1$. Finally, the symbols of the I and Q components are added to generate QAM QNSC symbols.

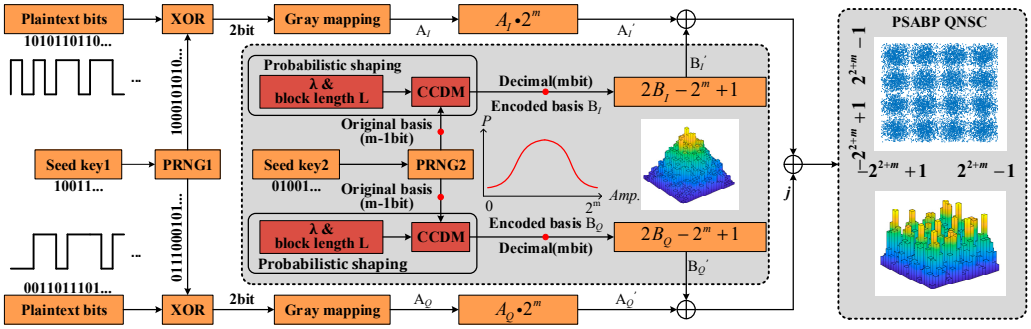

Figure 2. Schematic diagram of the principle of the PSABP 16QAM/QNSC scheme.

In traditional PS, the output is usually a symmetric bipolar 2^m-PAM signal, obtained from the asymmetric 2^{m-1}-PAM output of the CCDM with a half-Gaussian distribution [29]. However, the adjacent symbols with the smallest amplitudes, namely -1 and $+1$, have identical bit patterns except for the sign bit. This poses a challenge for the PSABP-QNSC scheme, as noise is unable to effectively obscure the difference between these adjacent symbols. To address this issue, the CCDM output in the PSABP-QNSC scheme should be constructed as a symmetric unipolar 2^m-PAM signal with a Gaussian distribution. This design ensures that adjacent bases differ in their encoded bits, especially in the least significant bit.

The constellations of PSABP QNSC signals affected by noise are shown in Figure 3. The probability distribution of the constellation of PSABP QNSC is a multi-peaked Gaussian distribution. The different SNR represents that the signals are affected by different intensities of noise. The QPSK, 16QAM and 64QAM have different robustness against noise. Therefore, the SNR is set to 10 dB and 5 dB in QPSK, and the SNR is set to 15 dB and 10 dB in 16QAM. The SNR is set to 20 dB and 15 dB in 64QAM. The constellations reveal that the adjacent PSABP QNSC symbols become indistinguishable due to noise masking. The illegal parties lacking a pre-shared key are unable to demodulate the PSABP QNSC symbols accurately. Even if illegal parties attempt to demodulate the PSABP QNSC symbols by treating them as low-order symbols (e.g., 16QAM), it remains impossible to recover the lower-position bits of the PSABP QNSC symbols. As a result, the receiver can hardly perform the XOR operation accurately to obtain the plaintext bits [8]. This attack methodology is equally suitable for traditional QNSC. Therefore, quantum noise has the potential to provide security for PSABP QNSC.

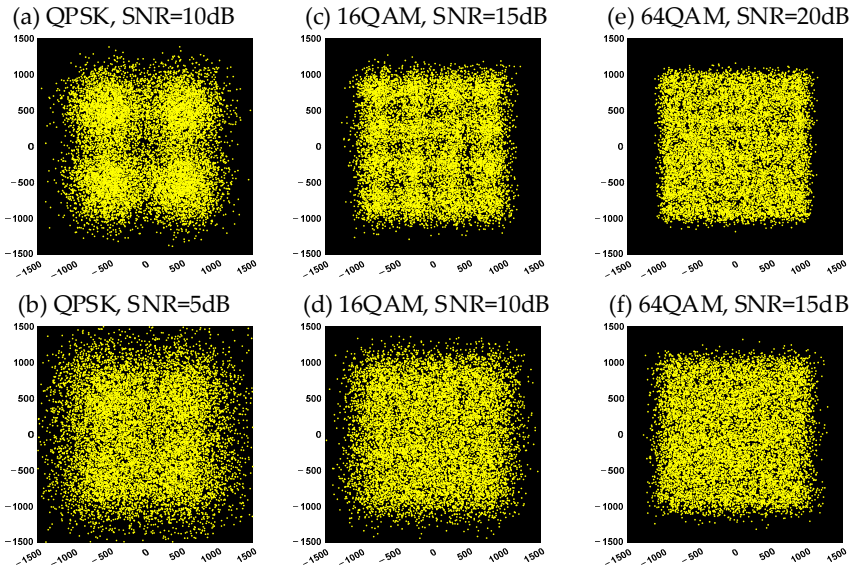

Figure 3. The constellations of PSABP QNSC signals with noise masking.

3. Transmission Performance Analysis

In our work, the two PRNGs and two sets of seed keys generate two sets of running keys. To simplify the analysis process, the running keys1 is used for the XOR operation, and the running keys2 is used for bases. The linear feedback shift register (LFSR) is usually used to generate pseudorandom numbers. Two LFSRs with lengths of 128 bits and 256 bits are employed as PRNG1 and PRNG2, respectively, each with a distinct seed key and primitive polynomial. For I or Q components, the probability of the QNSC symbol is expressed by the joint probability of bases $\boldsymbol{b}$ and symbol $\boldsymbol{a}$

$$P(\boldsymbol{c}_{(i,j)}) = P(\boldsymbol{a}_i, \boldsymbol{b}_j). \tag{5}$$

The subscripts $i = 1, 2, 3, \ldots, 2^n$ and $j = 1, 2, 3, \ldots, 2^m$ stand for the position of the element in the symbol sets A and B. According to Equation (5), the mean power of QNSC symbols (MP_{QNSC}) can be calculated as follows:

$$MP_{QNSC} = 2\sum_{i=1}^{2^n}\sum_{j=1}^{2^m}\left|\boldsymbol{c}_{(i,j)}\right|^2 P(\boldsymbol{c}_{(i,j)}). \tag{6}$$

When 2^m becomes sufficiently larger, MP_{QNSC} approaches an upper bound determined by the maximum amplitude in the I or Q component [18]. In this paper, the probability of bases is an MB distribution rather than a uniform distribution, which is

$$P(\boldsymbol{b}_j) = \frac{e^{-\lambda|b_j|^2}}{\sum_{j=1}^{2^m} e^{-\lambda|b_j|^2}}. \tag{7}$$

CCDM is employed to code the bases. The bases before CCDM coding are referred to as the original bases, whereas those after encoding are termed the encoded bases. The mean power of the PSABP QNSC symbols (MP_{PS}) is lower than that of uniform QNSC symbols ($MP_{uniform}$). Therefore, when the launch power remains unchanged, the minimum Euclidean distance of the PSABP QNSC symbol (MED_{PS}) increases accordingly. Traditional QNSC employs rectangular QAM modulation with a minimum Euclidean distance two. Therefore, MED_{PS} is calculated as follows:

$$MED_{PS} = 2\sqrt{\frac{MP_{uniform}}{MP_{PS}}}. \tag{8}$$

The QNSC signal's BER is naturally the plaintext's BER. The effective minimum Euclidean distance ($EMED$) is given in [21], which is the minimum Euclidean distance of QAM/QNSC signals under the same basis. Due to the expansion of constellation space, the $EMED$ deteriorates compared with the plaintext symbol, and the QNSC signal has the encryption penalty. The $EMED$ can be expressed as follows:

$$EMED = \frac{2^{m+1}}{2^{n+m}-1} h_{QNSC} \tag{9}$$

where h_{QNSC} is the maximal scalar value after power normalization in the I or Q component of the QNSC symbol. The h_{QNSC} is written as follows:

$$h_{QNSC} = \max\{|\boldsymbol{c_k}|\} \bullet \sqrt{\frac{MP_{QAM}}{MP_{uniform}}}, \tag{10}$$

$$MP_{QAM} = 2\sum_{i=1}^{2^n} |\boldsymbol{a_i}|^2 P(\boldsymbol{a_i}) \tag{11}$$

where MP_{QAM} is the mean power of the plaintext symbol and $P(\boldsymbol{a}_i) = \sum_{j=1}^{2^m} P(\boldsymbol{C}_{(i,j)})$. h_{QNSC} depends exclusively on two parameters: n (bit length of a plaintext symbol) and m (bit length of a basis). For example, the plaintext is modulated using QPSK, whereas the QNSC constellation is 256QAM ($n = 1$, $m = 3$, $2^{2(n+m)} = 256$). The mean powers of QPSK and 256QAM are 2 and 170, respectively ($MP_{QAM} = 2$, $MP_{uniform} = 170$). For the I component, the range of amplitude is $\pm1, \pm3, \pm5, \ldots, \pm15$ in 256QAM. $\boldsymbol{c_k}$ represents the amplitude of QNSC. Thus, $\max\{|c_k|\}$ is 15. According to Equation (10), $h_{QNSC} = 15 \times \sqrt{2/170} = 1.627$. Given a fixed value of n, h_{QNSC} is directly proportional to m, and approaches its theoretical upper bound as m becomes sufficiently large. The relational conclusions are also shown in [21].

The ratio of $EMED$ between QAM/QSNC and plaintext symbol is γ as a scalar and given by

$$\gamma = \frac{EMED}{2} = \frac{2^m}{2^{n+m}-1} h_{QNSC}. \tag{12}$$

Taking into account shaping gain, the final $EMED$ ($EMED_{final}$) is given by

$$\begin{aligned} EMED_{final} &= \gamma MED_{ps} \\ &= \sqrt{\frac{MP_{uniform}}{MP_{PS}}} \bullet \frac{2^{m+1}}{2^{n+m}-1} h_{QNSC} \end{aligned} . \tag{13}$$

In the standard constellation of rectangular QAM, it can be observed that $max\{|c_k|\} = 2^{n+m} - 1$. For example, in 256QAM, $max\{|c_k|\}$ is 15, and $n + m = 4$. Therefore, using Equation (10), $EMED_{final}$ is rewritten as follows:

$$EMED_{final} = 2^{m+1} \bullet \sqrt{\frac{MP_{QAM}}{MP_{PS}}}. \tag{14}$$

Equations (5)–(8) distinctly imply that the increase in MED_{PS} provided by the shaping gain is inherently limited. It is a reasonable assumption that MED_{PS} has an upper bound. When $\lambda \to +\infty$, only the central encoded bases with the highest probabilities are retained. Since each encoded basis remains unique, effective noise masking can still be achieved. Then, the encoded bases are used to encrypt plaintext symbols. It must be noted that each encoded basis must be composed of m bits are used to ensure the noise masking effects. Because noise with the same OSNR has different effects on 1101 and 1100000001, the lowest bit of the latter is more easily masked by noise. After being expanded into high-order ciphertext space, the shaped ciphertext symbol ($\boldsymbol{SC}$) is expressed as follows:

$$\begin{cases} \boldsymbol{SC_{2i-1}} = \boldsymbol{a_i} \bullet 2^m - (1,0) \\ \boldsymbol{SC_{2i}} = \boldsymbol{a_i} \bullet 2^m + (1,0) \end{cases} . \tag{15}$$

Note that all shaping ciphertext symbols are equiprobable occurrences in this case, according to Equation (5). Hence, the limit of $MP_{uniform}$ is written as follows:

$$\lim_{\lambda \to \infty} MP_{PS} = \frac{1}{2^n} \sum_{k=1}^{2^{n+1}} |\boldsymbol{SC_k}|^2. \tag{16}$$

Then, the bounds of MED_{PS} and $EMED_{final}$ can be calculated. Figure 4a shows this trend between the $EMED_{PS}$ and λ when $n = 1, m = 9$ and $n = 2, m = 8$, whose plaintext symbol formats are QPSK and 16QAM, respectively, and QNSC symbol format is 2^{20}QAM. Here, the theoretical bounds of MED_{PS} and $EMED_{final}$ are $2\sqrt{69{,}905/52{,}429}$ and $1024\sqrt{1/262{,}145}$ in QPSK. The bounds of MED_{PS} and $EMED_{final}$ are $2\sqrt{349{,}525/327{,}681}$ and $512\sqrt{5/327{,}681}$ in 16QAM. In the other cases, the theoretical bounds of $EMED_{final}$ approach two as m increases, as demonstrated in Figure 4b. From Figure 4, it is clearly seen that the proposed scheme can improve transmission performance and reduce the encryption penalty in the QNSC system.

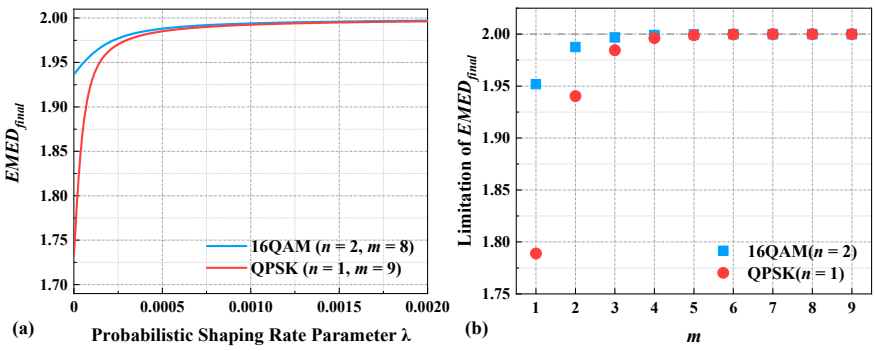

Figure 4. (**a**) The $EMED_{final}$ varies with λ and (**b**) the bounds value of $EMED_{final}$ varies with m.

4. Experimental Setup

We built an experimental setup for a coherent orthogonal frequency division multiplexing (OFDM) optical transmission, and Figure 5 shows the diagram of the experimental setup and DSP flows. Note that the single carrier system can also be used to demonstrate the feasibility of the proposed scheme. An external cavity laser (ECL) is applied to supply a stable laser with 10 dBm of power and 1550 nm of wavelength, and the linewidth is 32 kHz. An arbitrary waveform generator (AWG) with 10 GSa/s of sampling rate and 12 bits of resolution generates an electrical signal. The electrical signal, which is amplified by modulator drivers (MD), is loaded into the optical domain with an IQ modulator (IQ Mod.), and the output optical power is about −15 dBm. An erbium-doped fiber amplifier (EDFA) is used for maintaining the launch power of 0 dBm. After 160 km fiber link transmission, another EDFA is used to compensate for the power loss, which is 32 dB. To adjust the OSNR of the system, an EDFA offers extra ASE noise. A coherent receiver is adopted to recover the electrical signal. The local optical signal power is 10 dBm, which is provided by another ECL. A digital oscilloscope (DSO) captures the electrical signal at a sampling rate of 20 GSa/s. Two Eavesdropping points are placed in the output port of the IQ Modulator and the first EDFA to wiretap the optical signal with 100%, named points A and B. Specifically, point A denotes the eavesdropping position with the least ASE noise, while point B denotes the eavesdropping position with the highest optical signal power. Point B is the best eavesdropping point because of the highest optical power.

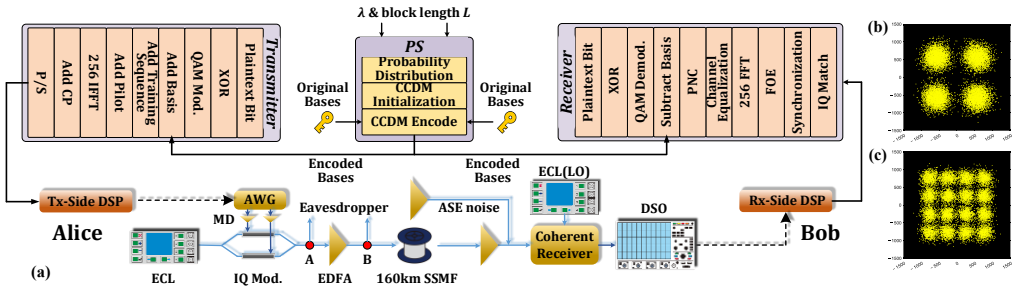

Figure 5. (**a**) Experimental setup and the constellations of (**b**) PSABP QPSK/QNSC and (**c**) PSABP 16QAM/QNSC at point A.

In the off-line DSP, the rate parameter λ and block length L are served as pre-shared parameters between Alice and Bob to initialize CCDM module. Due to satisfy $m - 1/m$ code rate, we set suitable λ and L, according to Table 2. λ and L constitute tunable parameters that enable transmission performance-security optimization in deployment scenarios. All original bases are regarded as a whole and then divided into different pieces according to L. The original bases with uniform distribution are encoded as encoded bases with a Gaussian distribution. In the first step of encryption, the plaintext bit is encrypted by the XOR operation in a bit-by-bit manner. Whereafter, QAM symbols with QPSK or 16QAM are modulated. In the second step of encryption, the encoded bases are added to the QPSK or 16QAM symbols. A 256-point FFT/IFFT is used for OFDM modulation. Only 128 subcarriers carry data, while 109 subcarriers for high frequency and 19 subcarriers for low frequency have zero padding to improve transmission performance [31]. Eight pilot subcarriers are inserted into an OFDM symbol to compensate phase noise of the lasers. The average value of the phase noise of eight pilot subcarriers is regarded as the phase noise of an OFDM symbol. Each 50 OFDM symbols used five training sequences. A total of 100 OFDM symbols are regarded as transmitted data, and the extra 10 OFDM symbols are used for channel estimation and equalization. Applying a cyclic prefix (CP) with 1/16 OFDM symbol length eliminates the inter-symbol interference caused by chromatic dispersion. An IQ match with the Gram–Schmidt orthogonalization (GSO) algorithm is

adopted to solve the IQ imbalance [32]. After performing symbol timing synchronization, frequency offset estimation (FOE), channel estimation and equalization, and phase noise compensation (PNC) are remedies for alleviating the influence of noise from the channel, transmitter, and receiver [33–35]. Then, the encoded basis is subtracted from the QNSC symbol, and an XOR is performed to recover the plaintext bit after QAM demodulation.

Table 2. Experimental parameters.

Plaintext	QNSC	L	λ
QPSK	2^{20}QAM	12,000	0.00011
16QAM	2^{20}QAM	12,000	0.000469

In the transmission experiment in our work, there is an assumption that a 15% overhead soft-decision forward error correction (SD-FEC) is employed. The symbol rate is 10 *GBaud*, and the net data rate is $2 \times 10 \times 120/256 \times 100/110 \times 16/17 \times 1/(1+15\%) \approx 7$ Gbit/s for QPSK and 14 Gbit/s for 16QAM (120/256: fraction of payload data subcarriers; 100/110: OFDM frame efficiency excluding the extra 10 OFDM training sequences; 16/17: CP efficiency for a CP length of 1/16; $1/(1+15\%)$: net coding efficiency after FEC overhead).

5. Experimental Results Analysis

In the OFDM system, an OFDM symbol consists of all subcarriers, and the time domain signal has a high peak-to-average power ratio (PAPR). The high PAPR will lead to nonlinearity distortion due to the deterioration of the signal-to-quantization noise ratio of the analog-to-digital converter and digital-to-analog converter. In addition, the efficiency of amplification is also decreasing. Hence, maintaining an outstanding PAPR is an important task in the OFDM system to avoid transmission performance degradation. The PAPR can be expressed by

$$PAPR = \frac{\max|x(t)|^2}{E\left\{|x(t)|^2\right\}} \tag{17}$$

where $x(t)$ is the time domain signal. There is a complementary cumulative distribution function (CCDF) to more felicitously represent PAPR performance, which is defined as a ratio of PAPR exceeding a certain threshold. Figure 6a shows the CCDF of PAPR of QPSK, traditional and PSABP QPSK/QNSC signals. Figure 6b shows the CCDF of PAPR of 16QAM, traditional and PSABP 16QAM/QNSC signals. It is obvious that the CCDF curves have no significant difference, which implies that those PAPR performances are almost the same.

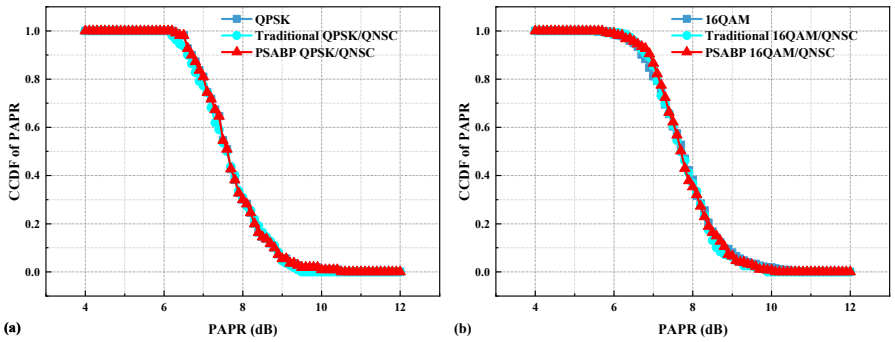

Figure 6. CCDF curves of (**a**) QPSK, traditional QPSK/QNSC, and PSABP QPSK/QNSC; and (**b**) 16QAM, traditional 16QAM/QNSC, and PSABP 16QAM/QNSC.

We experimentally measure the pre-FEC BER performance curves. We adjust the power compensation EDFA at the receiver end and the ASE noise source to control OSNR and the input power of the receiver. In addition, we also record the BER performances of QPSK, 16QAM and traditional QNSC schemes regarded as benchmarks. Figure 7 shows the experimental results in 160 km fiber links. In these scenarios, the QPSK and 16QAM have the best BER performance, while the traditional QNSC signals have the worst. As shown by theoretical analysis and experimental results, the PSABP QNSC scheme has BER performance second only to 16QAM signals in the same OSNR condition. Considering the SD-FEC coding with 15% overhead, the traditional QNSC schemes have encryption penalties of 0.6 dB and 0.41 dB, respectively, QPSK and 16QAM, while the PSABP QNSC schemes only have 0.16 dB and 0.14 dB, reducing them by 0.44 dB and 0.27 dB, in the 160 km fiber link scenario. We assume Eve cannot access the pre-shared seed keys (key1 and key2) but intercepts all transmitted optical signals. The signals are demodulated by Eve in the same way as Bob. Whereafter, Eve's BER performance curves are also shown in Figure 7, which maintain a fluctuation of about 0.5 in various OSNR conditions. Our experimental results indicate that the PSABP QNSC scheme can improve transmission performance compared with the traditional QNSC scheme and reduce the encryption penalty.

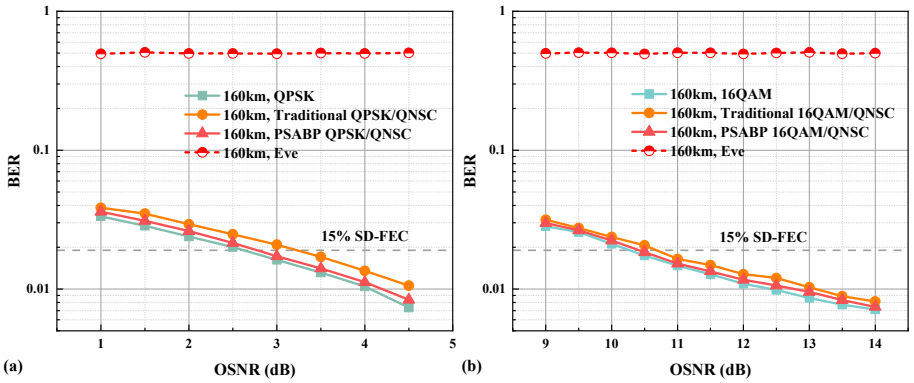

Figure 7. (**a**,**b**) The measured BER performance in the 160 km fiber scenario.

6. Security Analysis

In the QNSC system, there is a common attack assumption that Eve, without a pre-shared secret key, only demodulates ultra-high order QNSC symbols. Noise masking degrades Eve's decoding capability for QNSC symbols, manifesting as elevated symbol error ratios (SER). This SER serves as a key security indicator, with metrics including NMS and DFP characterizing the achievable security level. Elevated NMS and DFP values correspond to reduced mutual information at Eve, thereby enhancing system security. Considering the two-dimensional additive Gaussian white noise, the scope of the noise mask is a circle [36]. The NMS is defined as follows:

$$\Gamma = \pi\left(\frac{\sigma_I}{\Delta}\right)\left(\frac{\sigma_Q}{\Delta}\right) \tag{18}$$

where σ_I and σ_Q represent noise standard deviation I and Q components. The minimum Euclidean distance of QSNC after normalizing Δ is also expressed by [21]

$$\Delta = \frac{2h_{QNSC}}{2^{n+m}-1}. \tag{19}$$

The theoretical security stems from quantum noise, and the NMS of quantum noise is calculated by [21]

$$\Gamma_q = \frac{\pi}{3}\frac{eB_s}{P_s}\left(2^{n+m}-1\right)^2 \tag{20}$$

where B_s is signal bandwidth; P_s is the power of the optical signal; and e is the electric charge.

The above analysis is the calculation process of NMS of quantum noise in traditional QNSC. Compared with traditional QNSC, PSABP QSNC has a multi-peak Gaussian distribution, and the evaluation of NMS is more complex. On the one hand, PS affects the distance of adjacent ciphertext symbol points. On the other hand, some ciphertext symbol points may disappear. As shown in Figure 8, PS may reduce the number of constellation points. For example, 10 points with uniform distribution are shaped into six points with a Gaussian distribution. Only symbols with a small middle amplitude are retained. Particularly in practical systems, the frame length is limited, and therefore some symbol points with low occurrence probabilities may be absent. Therefore, constellation points that do not appear should not be considered in the NMS calculation for PSABP QNSC. Therefore, the calculation of NMS should be divided into two steps in PSABP QNSC.

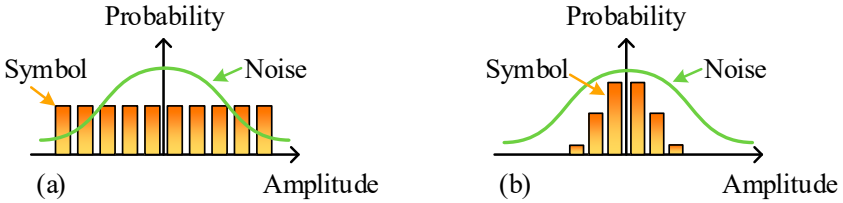

Figure 8. Schematic illustration of symbols masked by noise (**a**) traditional QNSC and (**b**) PSABP QNSC.

First step: Only the influence of Δ variation on the NMS is considered. In this step, it is assumed that applying PS only enlarges Δ while preserving all QNSC symbols. The first reason is that the signal power must remain invariant before and after PS, and the second reason is that a QNSC symbol still consists of $2(n+m)$ bits. Δ in PSABP QNSC is calculated by

$$\Delta_{PS} = \Delta\sqrt{\frac{MP_{uniform}}{MP_{PS}}}. \tag{21}$$

Therefore, Equation (20) in PSABP QNSC can be expressed by

$$\Gamma_{q-ps} = \frac{\pi}{3}\frac{eB_s}{P_s}\frac{MP_{PS}}{MP_{uniform}}\left(2^{n+m}-1\right)^2. \tag{22}$$

Second step: The impact of the disappeared QNSC symbols on the NMS is evaluated. The disappeared QNSC symbols should be removed after Equation (22), which causes NMS to be overestimated in PSABP QNSC.

If we regard QNSC symbol as 2^{2n}QAM, the constellation can be divided into 2^{2n} regions. The effect of adding m bits bases is to make 2^{2n}QAM randomly shift within its respective region. When the bases with Gaussian distribution are added to the 2^{2n}QAM symbols, the QNSC symbols of each region also appear in a Gaussian distribution. Overall, the constellation presents a multi-peaked Gaussian-like distribution.

Here, we conservatively assume that symbols near the region boundary remain within the original region despite the influence of quantum noise. Because quantum noise is a small noise. In each region, the maximum number of noise masked symbols is equal to the region's symbol count, which is the same as the number of base points. The effective base (EB) is used to represent the number of base points with a Gaussian distribution for I or

Q components. The EB is defined as bases with a frequency greater than one in a CCDM block length L:

$$EB = sum(L \bullet p(\boldsymbol{b}_j) \geq 1) \tag{23}$$

where $sum(.)$ is the sum of an array; and $(number1 \geq number2)$ return one when left value is not less than right value, or return zero. If the frequency of a base point within a block is less than one, this base point is considered absent and is excluded from the NMS calculation. The value of EB lies in the range from 2 to 2^m. Considering that there are I and Q components, the effective ciphertext symbol points ($ECSP$) is given by

$$ECSP = EB^2. \tag{24}$$

The $ECSP$ is defined as the number of bases remaining after the removal of QNSC symbol points that have disappeared. It serves the purpose of preventing the overestimation of NMS. Even under the effect of noise with large variance, the NMS remains within the bounds of $ECSP$. For example, if $ECSP$ is 256 in traditional QNSC, whereas it is 10 in PSABP QNSC. When the variance of quantum noise is large, the NMS of quantum noise is 200 in traditional QNSC, whereas it is only 10 in PSABP QNSC. When the variance of quantum noise is small, the NMS of quantum noise is 5 in traditional QNSC, whereas it may be 4 in PSABP QNSC, according to Equation (22). The NMS of quantum noise in PSABP QNSC should be determined jointly by quantum noise, the modulation format of QNSC symbol and $ECSP$.

The $ECSP$ curves with different shaping rate parameter λ are shown in Figure 9. In PSABP QPSK/QNSC, the shaping rate parameter λ is 0.00011 and m is nine. Then, EB is 392 and $ECSP$ is 153,664. Similarly, in PSABP 16QAM/QNSC, λ is 0.000464 and m is eight. Then, EB is 206 and $ECSP$ is 42,436.

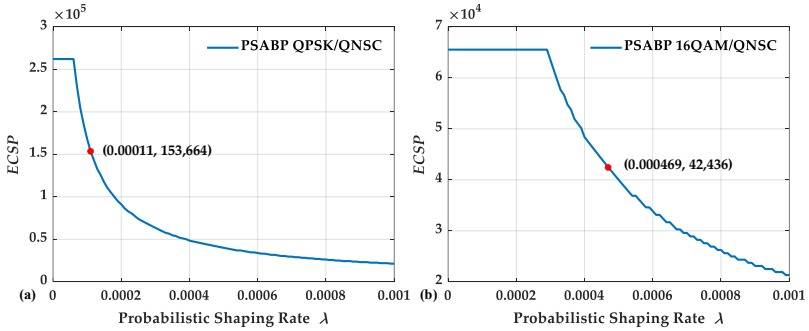

Figure 9. The $ECSP$ versus λ when PSABP QNSC symbol is 2^{20}QAM. The plaintext symbols are (**a**) QPSK and (**b**) 16QAM.

Finally, combining Equations (22) and (24), we can obtain the NMS of quantum noise in PSABP QNSC:

$$\Gamma_{q-ps} = \begin{cases} \frac{\pi}{3} \frac{eB_s}{P_s} \frac{MP_{PS}}{MP_{uniform}} (2^{n+m} - 1)^2 & , \Gamma_{q-ps} < ECSP \\ ECSP & , \Gamma_{q-ps} \geq ECSP \end{cases}. \tag{25}$$

When L is small, some high probability bases may not be contained in a block, thus constraining the upper bound of NMS calculated by Equation (25). To avoid this drawback as possible, L should be large enough to contain as many high probability bases in a block. Considering the specific scenario where the bases exhibit a uniform distribution, characterized by $P(\boldsymbol{b}_j) = 1/2^m$, the expected EB should be 2^m. Consequently, to satisfy this requirement, the L satisfies the condition $L \geq 2^m$.

In Figure 10, the NMS curves of quantum noise with different P_s are shown according to Equation (25). In traditional QSNC, the NMS merely depends on the quantum noise and the modulation format of QNSC. Thus, the traditional QPSK/QNSC and 16QAM/QNSC have a same NMS in our experiment. The signal bandwidth B_s is 10 GHz; the modulation format of QNSC is 2^{20}QAM, and the powers of optical signal are −15 dBm at point A and 0 dBm at point B. The NMSs of PSABP 16QAM/QNSC reach $ECSP$ only when the optical power is below −44 dBm. Because the effect of basis precoding is more evident in QPSK/QNSC, the corresponding decrease in NMS is more pronounced compared with that in 16QAM/QNSC. In Table 3, we record the NMS of all signals at point A and point B. At point A, the NMS induced by quantum noise is 53.18 for the PSABP 16QAM/QNSC signal and 44.35 for the PSABP QPSK/QNSC signal. At point B, the corresponding values decrease to 1.68 and 1.41, respectively. Therefore, the signals are effectively masked by quantum noise. It should be noted that the present experiments are limited by the optical signal power and signal bandwidth. Consequently, the NMS induced by quantum noise is lower than that reported in existing works.

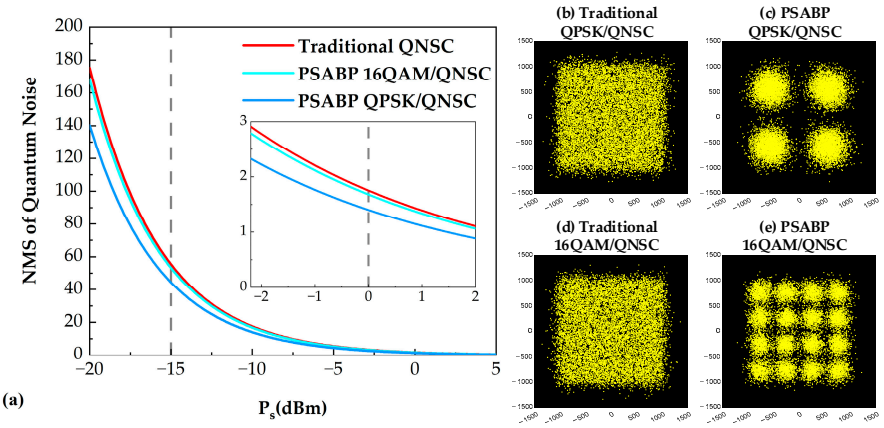

Figure 10. (**a**) The NMS of quantum noise versus P_s and the constellation before decryption of (**b**) traditional QPSK/QNSC, (**c**) PSABP QPSK/QNSC, (**d**) traditional 16QAM/QNSC, and (**e**) PSABP 16QAM/QNSC at point B.

Table 3. The NMS comparison when QNSC symbols are 2^{20}QAM.

	Traditional QNSC	PSABP QPSK/QNSC	PSABP 16QAM/QNSC
A	55.45	44.35	53.18
B	1.75	1.41	1.68

In the limit case of PS with $\lambda \to \infty$, the $ECSP$ is four. Therefore, the range of the NMS of PSABP QNSC is 0~4. If the power of the optical signal is attenuated to a small amount, the NMS of quantum noise is only four, but when the power of the optical signal is large enough, the NMS of quantum noise is reduced to zero. Although the limit case of PS has the best transmission performance, it is obviously less secure compared with traditional QNSC.

Herein, the effect of prior probabilities on the decision threshold is ignored because the probabilities of adjacent symbols are similar. Therefore, we can also calculate the DFP by [7]

$$DFP = 1 - \left(1 - \frac{2^{n+m}-1}{2^{n+m}} erfc\left(\frac{1}{\sqrt{2\Gamma_{p-qs}}}\right)\right)^2. \quad (26)$$

The DFP curves with different P_s are drawn in Figure 11. Because P_s is zero dBm at point B, the DFP are 69.72%, 63.77%, and 68.66% for traditional QNSC, PSABP QPSK/QNSC,

and PSABP 16QAM/QNSC, respectively. However, due to the greater quantum noise, the DFP of all signals increases significantly at point A, both exceeding 98%. The results show that, compared with the traditional QNSC scheme, the PSABP-QNSC scheme exhibits a slight reduction in security, as reflected by NMS decreases of 0.34 and 0.07, respectively. However, it still maintains effective resistance to eavesdropping and can protect the information.

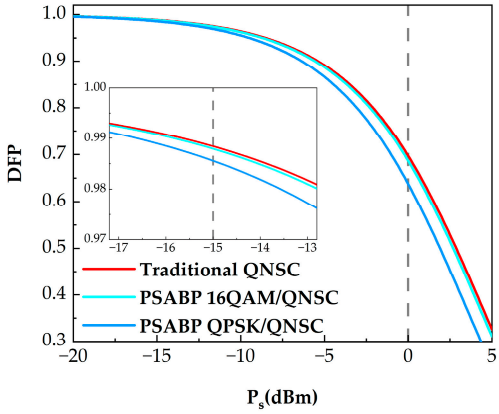

Figure 11. DFP curves versus P_s.

Assuming that Eve can eavesdrop under ideal conditions and remove all noise other than quantum noise, the NMS induced by quantum noise can be regarded as the theoretical security level, corresponding to the lower bound of system security. In practice, Eve's eavesdropping conditions are constraining. The other noise (e.g., ASE noise, thermal noise and quantization noise) can also mask signals to provide certain security. Therefore, it is harder for Eve to eavesdrop on useful information. The NMS of all noise can be calculated by Equations (18) and (19). Taking PSABP 16QAM/QNSC, for example, we measure the standard deviation of all noise $\overline{\sigma_I} = 0.1024$, and $\overline{\sigma_Q} = 0.1044$ at point B, as shown in Figure 12. Therefore, the NMS is 2808.84, and the DPF is 99.97% under the effects of all noise.

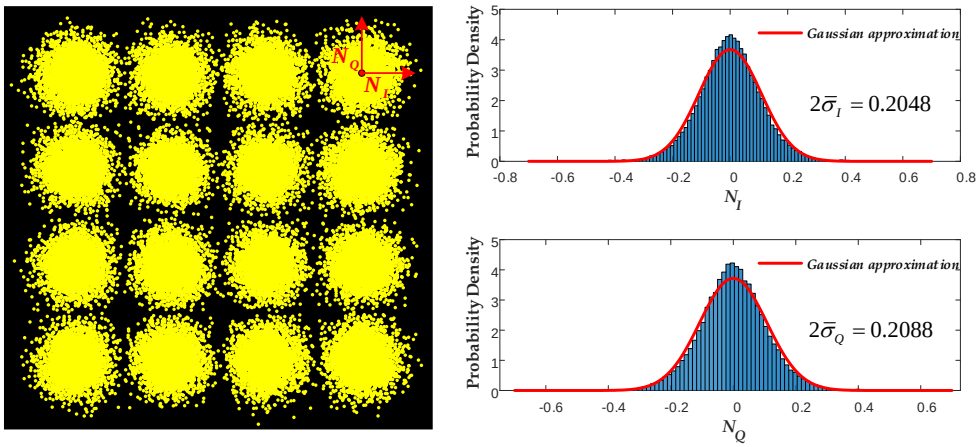

Figure 12. The constellation of PSABP 16QAM/QNSC after decryption and noise distribution in I/Q components.

It is non-negligible that the QNSC system combines physical encryption and mathematical encryption, which are masking effect of noise and XOR operation [7]. The NMS and DFP represent physical factors. To intercept a plaintext bit, Eve must accurately XOR operation. Information leakage in PSABP QNSC systems can be quantified through mu-

tual information analysis, providing a theoretical foundation for security evaluation. The mutual information of Eve can be calculated by [37]

$$\begin{aligned} C_{Eve} &= 1 - H(BER_{Eve}) \\ &= 1 + BER_{Eve}\log_2 BER_{Eve} + (1 - BER_{Eve})\log_2(1 - BER_{Eve}) \end{aligned}. \quad (27)$$

Under noise masking, the lowest bit of each symbol experiences distortion, rendering it inherently resistant to accurate detection by Eve. When only quantum noise is considered, the symbol error probability d for either I or Q component is given by:

$$d = \frac{2^{n+m} - 1}{2^{n+m}} erfc\left(\frac{1}{\sqrt{2\Gamma_{p-qs}}}\right). \quad (28)$$

Considering that the lowest bits of adjacent symbols alternate between zero and one. When Eve detects symbols with error probability d, the probability of correctly detecting the lowest bit reduces to 0.5, statistically equivalent to random guessing. On the contrary, when Eve detects symbols with correct probability $1 - d$, the probability that Eve obtains the correct lowest bit is 1. Therefore, the detection correct probability of the lowest bit is $1 \times (1 - d) + 0.5 \times d = 1 - 0.5d$, and the detection error probability of the lowest bit is $0.5d$. The lowest bit is used to XOR with high bit of a QNSC symbol. Where only quantum noise is taken into account, the BER can be approximately regarded as $0.5d$. Given the independence of I/Q components, the overall BER is determined by the average of the individual component BERs. The overall BER is $(0.5d + 0.5d)/2 = 0.5d$. Therefore, under the masking effect of quantum noise, the mutual information of Eve can be expressed by

$$C_{Eve} = 1 + 0.5d\ \log_2 0.5d + (1 - 0.5d)\log_2(1 - 0.5d). \quad (29)$$

It should be noted that Equation (29) is an idealized analytical result, since it does not include practical channel impairments such as phase noise, ASE noise, and fiber nonlinearities, which may introduce joint error propagation and correlation. We record the mutual information of Eve versus power P_s with different schemes in Figure 13. The results reveal that PSABP QPSK/QNSC exhibits the highest information leakage (0.28 bit), exceeding traditional QNSC (0.231 bit), while the leakage of PSABP 16QAM/QNSC with 0.239 bit shows a marginal difference from traditional QNSC. In practice, phase noise, ASE noise, and fiber nonlinearities may introduce error correlation and joint propagation effects, so that Eve's practical BER may deviate from the idealized value $0.5d$. Therefore, we measure the BER of Eve at point B, and the mutual information is calculated by Equation (27), as 1.78×10^{-4} bits, 1.85×10^{-4} bits and 2.2×10^{-4} bits, which are, respectively, traditional QNSC, PSABP 16QAM/QNSC, and PSABP QPSK/QNSC. The results can reflect the practical security performance of the proposed schemes under realistic transmission conditions. In [37], the mutual information leakage is less than 2×10^{-4} bit, while our results only exhibit a slight difference compared with this value.

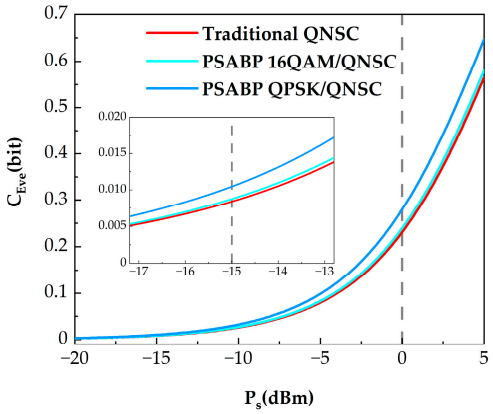

Figure 13. The mutual information of Eve versus P_s, under the masking effect of quantum noise.

7. Discussion

At present, the transmission performance and security are the focus of optical communications. However, the implementation of high security usually results in a transmission performance penalty. Traditional QAM/QNSC has been proven to have an encryption penalty due to the deterioration of *EMED*. In practical scenarios, it depends on practical demands whether better transmission performance or higher security should be chosen. The PSABP QNSC sacrifices acceptable security in exchange for better transmission performance, which can expand the application scope of QNSC. The PSABP QNSC is proposed to provide an alternative method of reducing penalties for satisfying the security requirements of optical communications in special scenarios. The transmission performance penalty caused by secure encryption is often the focus of communication equipment manufacturers. Particularly for long-distance transmission or under equipment aging scenarios, secure communication systems may operate under OSNR-limited marginal conditions. In such cases, the encryption penalty may determine whether secure transmission can still satisfy the required performance threshold. Equivalently, this improvement can be interpreted as additional system margin for secure transmission. Therefore, the reduction of 0.44 dB and 0.27 dB in encryption penalty for QPSK and 16QAM, respectively, is of practical significance. Moreover, the shaping parameter λ in the PSABP QNSC scheme enables a controllable trade-off between security and transmission performance, allowing the system to adapt to different operating conditions and threat levels.

8. Conclusions

We experimentally demonstrate a PSABP QNSC scheme on a coherent optical communication platform over 160 km SSMF. In the proposed scheme, Gaussian distributed bases are used to generate QNSC symbols, which alleviates the encryption penalty and improves the transmission performance. We also theoretically investigate the shaping gain boundary of PSABP QNSC. In the 160 km SSMF scenario, the proposed scheme achieves encryption penalties of 0.16 dB and 0.14 dB for QPSK and 16QAM, respectively, corresponding to reductions of 0.44 dB and 0.27 dB compared with the traditional QNSC. In addition, an optimized NMS calculation method is proposed to evaluate the security of this scheme more accurately. The mutual information of Eve under different signal power conditions is also analyzed. At the eavesdropping position with the highest optical signal power, the proposed scheme achieves NMS values of 1.41 and 1.68, corresponding DFP values of 63.77% and 68.66%, and mutual information leakage of 0.28 bit and 0.239 bit for QPSK and 16QAM, respectively. These results indicate that the proposed scheme improves transmission performance while preserving the security benefit provided by quantum noise

masking. In practical environments, other factors such as ASE noise, thermal noise and nonlinear effects may also affect the practical security performance.

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

Funding: This research was funded by NSFC project (62471063), the Fundamental Research Funds for the Central Universities, BUPT Excellent Ph.D. Students Foundation (CX20242035) and BUPT-CMCC Joint Innovation Center.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The original contributions presented in this study are included in the article. Further inquiries can be directed to the corresponding authors.

Acknowledgments: Portions of this work were presented at the International Conference on Optical Network Design and Modelling (ONDM) 2023 in the paper entitled "Basis Precoding Based on Probabilistic Constellation Shaping in QAM/QNSC."

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

References

1. Li, G. Recent advances in coherent optical communication. *Adv. Opt. Photon.* **2009**, *1*, 279–307. [CrossRef]
2. Nair, R.; Yuen, H.P.; Corndorf, E.; Eguchi, T.; Kumar, P. Quantum-noise randomized ciphers. *Phys. Rev. A* **2006**, *74*, 052309. [CrossRef]
3. Nakazawa, M.; Yoshida, M.; Hirooka, T.; Kasai, K. QAM quantum stream cipher using digital coherent optical transmission. *Opt. Express* **2014**, *22*, 4098–4107. [CrossRef] [PubMed]
4. Li, J.; Han, C.; Ye, N.; Pan, J.; Yang, K.; An, J. Instant Positioning by Single Satellite: Delay-Doppler Analysis Method Enhanced by Beam-Hopping. *IEEE Trans. Veh. Technol.* **2025**, *74*, 14418–14431. [CrossRef]
5. Kikuchi, K. Fundamentals of Coherent Optical Fiber Communications. *J. Light. Technol.* **2015**, *34*, 157–179. [CrossRef]
6. Timo, P.; Hoffmann, S.; Noé, R. Hardware-efficient coherent digital receiver concept with feedforward carrier recovery for M-QAM constellations. *J. Light. Technol.* **2009**, *27*, 989–999. [CrossRef]
7. Tanizawa, K.; Futami, F. Digital coherent PSK Y-00 quantum stream cipher with 2^{17} randomized phase levels. *Opt. Express* **2019**, *27*, 1071–1079. [CrossRef]
8. Zhang, M.; Li, Y.; Zhu, K.; Wei, S.; Li, Y.; Zhao, Y.; Zhang, J. Experimental Demonstration of An Efficient Correlation Attack Method in 300 km QAM/QNSC Transmission. In Proceedings of the Optical Fiber Communication Conference (OFC) 2024, San Diego, CA, USA, 24–28 March 2024; p. Th3B.2.
9. Sun, J.; Jiang, L.; Yi, A.; Pan, W.; Yan, L. Security analysis of quantum noise stream cipher systems under quantization-attack. *Photon. Res.* **2026**, *14*, 411–425. [CrossRef]
10. Iwakoshi, T. Example of Guessing Probability on Secret Key by Known-Plaintext Attack on Y00 Quantum Stream Cipher. In *Frontiers in Optics/Laser Science*; OSA Technical Digest; Optica Publishing Group: Washington, DC, USA, 2018; paper JTu2A.60. [CrossRef]
11. Futami, F.; Tanizawa, K.; Kato, K. Y-00 Quantum-Noise Randomized Stream Cipher Using Intensity Modulation Signals for Physical Layer Security of Optical Communications. *J. Light. Technol.* **2020**, *38*, 2774–2781. [CrossRef]
12. Zhu, H.; Liu, Z.; Chen, S.; Xu, X.; Li, F. Optical stealth communication based on quantum noise stream ciphered amplified spontaneous emission light. *Opt. Express* **2023**, *31*, 3595–3605. [CrossRef]
13. Futami, F.; Tanizawa, K.; Kato, K. Experimental Demonstration of Quantum Deliberate Signal Randomization for Y-00 Quantum Noise Stream Cipher. In *Conference on Lasers and Electro-Optics*; Technical Digest Series; Optica Publishing Group: Washington, DC, USA, 2022; paper JW3B.107. [CrossRef]
14. Xu, Y.; Gao, M.; Fei, Y.; Chen, B.; Shao, W. Diffusion-assisted quantum noise stream cipher for physical layer security in UFMC. *Opt. Laser Technol.* **2023**, *171*, 110407. [CrossRef]

15. Wei, S.; Li, Y.; Zhu, K.; Lei, C.; Li, Y.; Pan, M.; Wang, W.; Zhao, Y.; Zhang, J. Physical Layer Secure Key Distribution Based on Artificial Amplitude Noise in QAM/QNSC Optical Communication Systems. *IEEE Commun. Lett.* **2023**, *27*, 2288–2292. [CrossRef]
16. Tanizawa, K.; Futami, F. Ultra-long-haul digital coherent PSK Y-00 quantum stream cipher transmission system. *Opt. Express* **2021**, *29*, 10451–10464. [CrossRef]
17. Lei, C.; Zhang, J.; Li, Y.; Zhao, Y.; Wang, K.; Liu, S.; Wang, B.; Gao, H.; Li, J. 16 QAM Quantum Noise Stream Cipher Coherent Transmission Over 300 km Without Intermediate Amplifier. *IEEE Photon. Technol. Lett.* **2021**, *33*, 1002–1005. [CrossRef]
18. Chen, Z.; Li, Y.; Zhu, K.; Li, Y.; Wei, S.; Zhao, Y.; Zhang, J. Low Encryption Penalty LEO-to-Earth Secure Laser Communication Based on Quantum Noise Stream Cipher. In Proceedings of the 2025 23rd International Conference on Optical Communications and Networks (ICOCN), Zhangjiajie, China, 28–31 July 2025; pp. 1002–1005. [CrossRef]
19. Xie, Y.; Huang, X.; Xu, G.; Xiao, J.; Shi, M.; Hu, W.; Yi, L. Implementation of 400 Gbps quantum noise stream cipher encryption for 1520 km fiber transmission using end-to-end deep learning. *Opt. Lett.* **2025**, *50*, 3808–3811. [CrossRef]
20. Sun, J.; Jiang, L.; Yi, A.; Feng, J.; Deng, X.; Pan, W.; Luo, B.; Yan, L. Experimental demonstration of 201.6-Gbit/s coherent probabilistic shaping QAM transmission with quantum noise stream cipher over a 1200-km standard single mode fiber. *Opt. Express* **2023**, *31*, 11344–11353. [CrossRef]
21. Li, Y.; Li, Y.; Zhu, K.; Wang, W.; Zhao, Y.; Zhang, J. Analysis of the encryption penalty in a QAM-based quantum noise stream cipher. *Opt. Express* **2023**, *31*, 19006–19020. [CrossRef]
22. Askari, M.T.; Lampe, L.; Mitra, J. Probabilistic Amplitude Shaping and Nonlinearity Tolerance: Analysis and Sequence Selection Method. *J. Light. Technol.* **2023**, *41*, 5503–5517. [CrossRef]
23. Civelli, S.; Parente, E.; Forestieri, E.; Secondini, M. On the Nonlinear Shaping Gain with Probabilistic Shaping and Carrier Phase Recovery. *J. Light. Technol.* **2023**, *41*, 3046–3056. [CrossRef]
24. Hossain, M.; Böcherer, G.; Rahman, T.; Wettlin, T.; Stojanović, N.; Calabrò, S.; Pachnicke, S. Probabilistic Shaping for High-Speed Unamplified IM/DD Systems With an O-Band EML. *J. Light. Technol.* **2023**, *41*, 5373–5382. [CrossRef]
25. Luo, H.; Zhong, L.; Dai, X.; Cheng, M.; Yang, Q.; Deng, L.; Liu, D. DAC/ADC-free 4 × 12.9 Gbit/s 65,536-level quantum noise stream cipher secure optical WDM transmission based on delta-sigma modulation. *Opt. Lett.* **2022**, *47*, 5104–5107. [CrossRef]
26. Luo, H.; Zhang, Z.; Dai, L.; Wu, D.; Yang, Q.; Deng, L.; Liu, D.; Dai, X.; Cheng, M. Physical-Layer Secure Optical Transmission Based on Randomized Quantization Noise. *IEEE Trans. Inf. Forensics Secur.* **2025**, *20*, 10937–10950. [CrossRef]
27. Luo, H.; Zhang, Z.; Dai, L.; Zhong, L.; Yang, Q.; Deng, L.; Liu, D.; Dai, X.; Gao, X.; Cheng, M. Device-compatible ultra-high-order quantum noise stream cipher based on delta-sigma modulator and optical chaos. *Commun. Eng.* **2024**, *3*, 27. [CrossRef]
28. Wei, S.; Liu, S.; Lei, C.; Li, Y.; Wang, W.; Zhao, Y.; Li, Y.; Zhang, D.; Yang, H.; Li, H.; et al. Basis Precoding Based on Probabilistic Constellation Shaping in QAM/QNSC. In Proceedings of the 2023 International Conference on Optical Network Design and Modeling (ONDM), Coimbra, Portugal, 8–11 May 2023; pp. 1–3. [CrossRef]
29. Schulte, P.; Bocherer, G. Constant Composition Distribution Matching. *IEEE Trans. Inf. Theory* **2015**, *62*, 430–434. [CrossRef]
30. Cho, J.; Winzer, P.J. Probabilistic Constellation Shaping for Optical Fiber Communications. *J. Light. Technol.* **2019**, *37*, 1590–1607. [CrossRef]
31. Li, F.; Li, X.; Yu, J.; Chen, L. Optimization of training sequence for DFT-spread DMT signal in optical access network with direct detection utilizing DML. *Opt. Express* **2014**, *22*, 22962–22967. [CrossRef] [PubMed]
32. Fatadin, I.; Savory, S.J.; Ives, D. Compensation of Quadrature Imbalance in an Optical QPSK Coherent Receiver. *IEEE* Photon.-Technol. Lett. **2008**, *20*, 1733–1735. [CrossRef]
33. Schmidl, T.M.; Cox, D. Robust frequency and timing synchronization for OFDM. *IEEE Trans. Commun.* **1997**, *45*, 1613–1621. [CrossRef]
34. Ozdemir, M.K.; Arslan, H. Channel estimation for wireless ofdm systems. *IEEE Commun. Surv. Tutor.* **2007**, *9*, 18–48. [CrossRef]
35. Yi, X.; Shieh, W.; Tang, Y. Phase Estimation for Coherent Optical OFDM. *IEEE Photon. Technol. Lett.* **2007**, *19*, 919–921. [CrossRef]
36. Tanizawa, K.; Futami, F. Photonic-Assisted Secure Millimeter Wave Communication with Quantum Noise Randomized Stream Cipher. *J. Light. Technol.* **2024**, *42*, 7745–7751. [CrossRef]
37. Zhang, L.; Deng, Q.; Zhang, H.; Yang, Z.; Pang, X.; Bobrovs, V.; Popov, S.; Wu, Y.; Yu, X.; Ozolins, O.; et al. Quantum Noise Secured Terahertz Communications. *IEEE J. Sel. Top. Quantum Electron.* **2022**, *29*, 8400110. [CrossRef]