Basis Precoding Based on Probabilistic Constellation Shaping in QAM/QNSC

Shuang Wei[1†], Sheng Liu[2†], Chao Lei[1†], Yajie Li[1], Wei Wang[1], Yongli Zhao[1], Yunbo Li[2], Dechao Zhang[2], Hui Yang[1], Han Li[2] and Jie Zhang[1*]
[1]School of Electronic Engineering, Beijing University of Posts and Telecommunications, China, *jie.zhang@bupt.edu.cn
[2]Department of Fundamental Network Technology, China Mobile Research Institute, Beijing, China

***Abstract*—Quantum noise stream cipher (QNSC) is a physical-layer encryption approach for optical communications, and its security barrier is the "basis" that is used as the secret-key for symbol encryption. Regarding the fact that the basis is actually transmitted through the fiber, we propose a basis precoding scheme based on probabilistic constellation shaping, to better conceal the basis into the noise for security enhancement. Experimental results show our scheme can improve the security of the QAM/QNSC system in terms of Eve's symbol error ratio.**

Keywords—quantum noise stream cipher, probabilistic constellation shaping, basis

I. Introduction

The optical network with high bandwidth and low delay meets the demand of abundant information transmission. In recent years, with the flourishing development of quantum computing, the encryption schemes based on mathematical complexity hardly meet the protection needs, and the security in optical networks faces greater challenges. Many researchers are engaged in the search for more secure encryption technologies. The physical layer security technology has become one of the current hot spots [1]. Y-00 quantum noise stream cipher (QNSC) is a popular physical layer security approach, which combines the advantages of both the ineluctable quantum noise and mathematical cryptography [2]. With Y-00, the original low-order plaintext signals at the legal transmitter are mapped to high-order ciphertext by coding with pre-shared secure keys, which is also referred to as the "basis". Following the Y-00 coding protocol, the pre-shared key will be hidden in the quantum noise, and thus the ciphered signals can only be decrypted by the legitimate receiver with the pre-shared basis.

In the context of physical-layer security, capacity and security are two important metrics. Regarding the transmission capacity, experiments demonstrated a 10Tbit/s secure physical layer transmission using a combination of QAM/QNSC and injection-locked WDM techniques [3]. Focusing on the long-haul system without intermediate amplifiers, a 16 QAM/QNSC transmission system over 300km fiber was reported, and the product of distance and data rate has reached 10.2Tbit/s·km [4]. In addition, in terms of security, the fast correlation attack (FCK) can be prevented by maintaining a high-level noise mask and timely updating the seed keys [5]. In the above studies, the security degree of QNSC is evaluated in terms of the number of masked signals (NMS) or symbol error ratio (SER) for the eavesdropper (Eve). The larger NMS or the higher SER for Eve means a higher security level of the system. There are two typical ways to improve these two metrics, i.e., strengthening the noise effect of the system [6] and reducing the Euclidean distance between adjacent ciphertext signal symbols.

In fact, the above two metrics are valid only under the assumption that the pre-shared keys or the basis cannot be tracked by Eve. Otherwise, Eve will also be able to decrypt the ciphertext, just like a legitimate receiver. Therefore, the security of the basis is another fundamental factor for the overall security of a QNSC system. However, even though the QNSC system tries to hide the basis in the quantum noise, one risky fact is that the basis is actually coded into the ciphertext and transmitted through the fiber [7]. Therefore, the security of the basis itself is another important issue that needs to be addressed and it is worth exploring the approaches to enhance the security of the basis in QNSC.

Similar to the methodology for improving the security of the ciphertext symbols, one possible approach for securing the basis is to strengthen the noise's masking effect on the basis. In a traditional QNSC system, the basis with uniform distribution does not match noise so that the basis cannot be completely masked by noise. In this case, probabilistic constellation shaping (PCS), which can shape the probability distribution of signal symbols in the constellation [8], might be a promising technique for manipulating the distribution of the basis. Based on such advantages of PCS, this work investigates the ways for shaping the distribution of basis in the QNSC system, with the aim to tune the noise's masking effect on the basis. Besides, PCS improves the transmission performance of QNSC and reduces the performance loss caused by encryption algorithm.

This paper proposes a PCS-based basis encoding scheme to shape the distribution of basis to be matched with the distribution of noise and make the basis better masked with noise. We adopt the constant composition distribution matching (CCDM) algorithm to shape the basis following the desired distribution (e.g., Gaussian-like or Trapezoidal distributions). The proposed scheme is implemented in an 8.5Gbit/s (10Gbaud/s ×2×1/2×(1-15%)) QAM/QNSC system over 300km ultra-low loss fiber (ULF). Experimental results show that our proposed scheme can improve the OSNR by 0.9 dB, Eve's basis error ratio by 2.9E-4, and Eve's SER by 5.8E-5 in the optimal condition.

II. QNSC with PCS-based Basis Shaping

This section introduces the CCDM algorithm briefly and designs the PCS-based basis shaping and Y-00 encryption schemes for the QNSC system.

978-3-903176-54-6 © 2023 IFIP

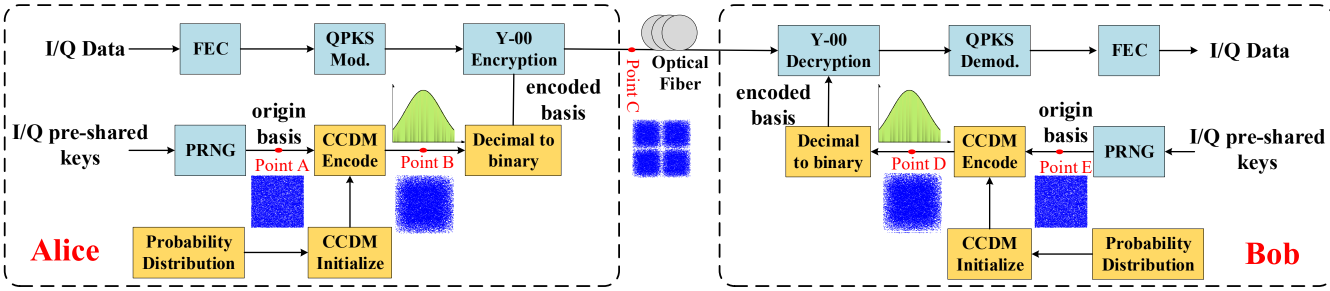

Fig. 1: Flow chart of QNSC with Gaussian-like PCS-based basis.

A. PCS algorithm

CCDM is a famous PCS algorithm and it can convert independent and equiprobable binary bit sequences into a series of symbols with desired probability distributions. As a rule, output symbols of CCDM follow Maxwell-Boltzmann (MB) distribution, which is a Gaussian-like distribution. The usage of MB distributions can approximate the capacity limit of a channel with the additive white Gaussian noise, by gathering constellation points towards the center area. In contrast to the conventional PCS, which employs the half-MB distribution for amplitude before adding a +1/-1 sign, we choose the Gaussian-like and Trapezoidal shape distributions for amplitude with CCDM algorithm.

B. PCS-based Basis Shaping Scheme

Following the Y-00 protocol, the legitimate transmitter and receiver have the pre-shared keys. The shared keys are used to generate a set of origin keys using the pseudo-random number generator (PRNG). After CCDM encoding, the origin keys will be transformed into a set of symbols that follow the Gaussian-like or Trapezoidal distributions. Each symbol from the CCDM output is further transformed into binary bits, which will be used as the final basis for Y-00 encryption. In this way, the basis symbol points are concentrated in the center area of the constellation diagram, and thus the noise will be better masked with basis points.

Note that the basis shaping is performed at both the legitimate transmitter and receiver sides. Therefore, the legitimate receiver, Bob can also obtain exactly the same final basis following the same CCDM encoding process with the same distribution settings. The constellation diagrams at point A/E and point B/D in Fig. 1 illustrate the basis before and after Gaussian-like PCS at the transmitter and receiver sides.

C. Y-00 En/Decoding with Shaped Basis

With Gaussian-like distribution as an example, Fig. 1 further illustrates the overall Y-00 encoding and decoding process based on the final basis from the CCDM module. At the transmitter side, before the Y-00 encoding, Alice first encodes the plaintext data with the forward error correction (FEC) algorithm and modulates the data into QPSK format. The QPSK signal is further encrypted with the final basis following the Y-00 protocol. The constellation diagram at point C in Fig. 1 shows the distribution of the cyphertext symbols with the final basis under Gaussian-like distribution. It is notable that the ciphertext symbols are also no longer evenly distributed.

As discussed, the legitimate receiver also has the same final basis, and it can recover the plaintext correctly by performing Y-00 decoding, QPSK demodulation, and FEC decoding.

III. Experimental Setup and Results

To verify the performance of the proposed scheme, we construct an experiment setup, as shown in Fig. 2. At the transmitter side, the arbitrary waveform generator (AWG) generates a signal with 300mV according to the output of DSP. An external cavity laser (ECL) is employed to maintain a stable laser with 10dBm of optical power at 1550nm. An I/Q modulator modulates electrical signal to optical signal. For the CCDM module inside the DSP part, we adopt the Gaussian-like and Trapezoidal distributions as two candidates to perform the PCS.

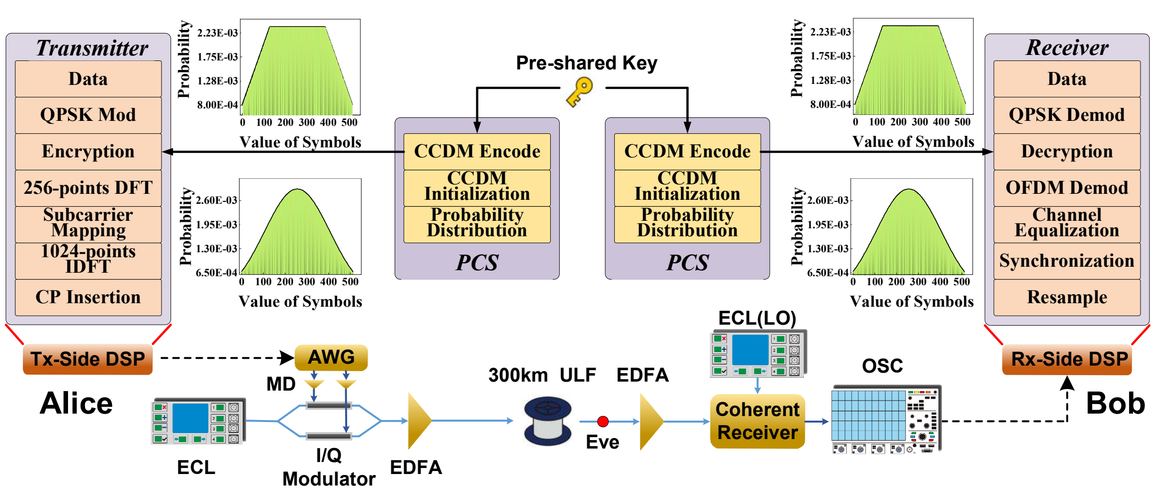

Fig. 2: Experimental setup.

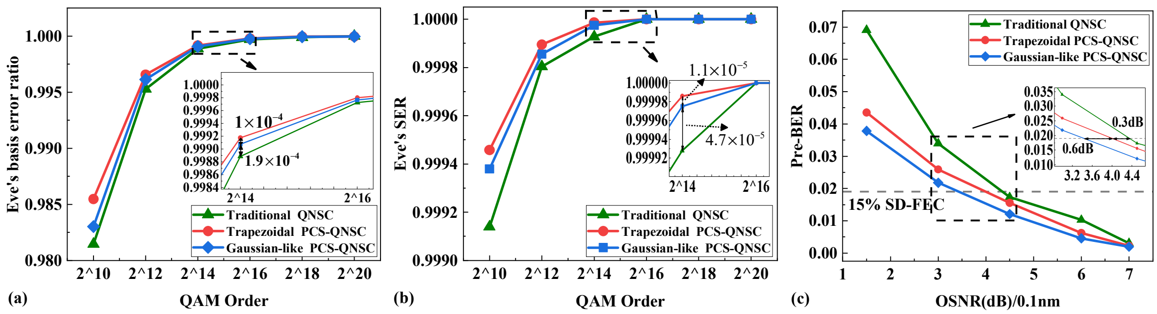

Fig. 3. (a) Eve's SER and (b) Eve's basis error ratio as a function of the QAM order (c) Pre-BER as the function of the OSNR of the 2^20 QAM/QNSC

After encrypting the plaintext data with the shaped basis, a DFTs-OFDM with 256-points DFT and 1024-points IDFT is adopted to reduce the peak-to-average power ratio of the system. Finally, the ciphertext symbols are dumped into a 300km of ULF channel without any intermediate amplifier. At the receiver side, the input power of the receiver is set to -5.3dBm. The sampling rate of the digital oscilloscope (OSC) is set to 40GSa/s. In the receiver's DSP part, the CCDM module uses the same parameters as the transmitter to generate the same shaped basis for further decoding from ciphertext symbols to plaintext. We experimentally demonstrated an 8.5Gbit/s QAM/QNSC system and measured Eve's basis error ratio and SER under various QAM orders, ranging from 2^{10} to 2^{20}. We also measure the bit error ratio (BER) performance with the mapping space size (i.e., QAM order) fixed at 2^{20}. Note that, with QPSK signal as the plaintext, the constellation size for the basis is 2^{18} for the 2^{20} QAM/QNSC system.

Fig. 3 (a) and (b) depict the basis error ratio and SER of Eve as a function of the QAM order. The eavesdropping point is located at the output end of the fiber, at which Eve can imitate Bob. It is observed that the basis shaping scheme with Trapezoidal distribution achieves a higher basis error ratio and SER when the QAM order is lower than 2^{16}. Gaussian-like distribution can also improve Eve's basis error ratio and SER, but the improvement is not as significant as the Trapezoidal distribution under lower QAM orders. That is, the Trapezoidal distributed basis symbol points are better masked by the noise (larger number of masked bases means higher security). This is because the basis symbol points of the Trapezoidal distribution are more concentrated in the center area of the constellation diagram and have lower average power than the Gaussian-like distribution.

Fig. 3 (c) plots uncorrected BER, namely pre-BER, under different OSNR conditions within a range from 1.5 to 7.5dB. The proposed schemes achieve error-free transmission when OSNR is larger than 4.5dB. Compared to the traditional QNSC without basis shaping, the PCS-based basis shaping scheme for a 2^{20} constellation with the Gaussian-like and Trapezoidal distribution achieves 0.9dB and 0.3dB OSNR improvement (with 15% overhead soft decision FEC). Moreover, the scheme with Gaussian-like distribution achieves a better BER performance than the Trapezoidal-like distribution when the QAM order is 2^{20}. The reason is that the Gaussian-like distributed constellation achieves the lowest average power and the largest Euclidean distance under the same launch power.

In summary, by concentrating the basis symbols in the center area of the constellation diagram, the proposed PCS-based basis shaping scheme can enhance the security performance of QNSC in terms of Eve's basis error ratio and SER and achieve OSNR improvement. However, there's a fly in the ointment: the order of basis is generally exceeding high to ensure security, which greatly increases the complexity of PCS algorithm. How to reduce the complexity of the algorithm is also the focus of our future work.

IV. Conclusions

This paper proposed a basis precoding scheme based on PCS in QAM/QNSC to conceal the basis in the noise for security enhancement. Experimental results show that the proposed scheme can improve OSNR by 0.9 dB with 15% overhead SD-FEC, while increase the basis error ratio of Eve by 2.9E-4 and the SER of Eve by 5.8E-5 in the 2^{14} QAM/QNSC.

Acknowledgment

This work is supported in part by NSFC (Grant No. 61831003, 62101063, 61901053, and 62021005), the BUPT-CMCC Joint Innovation Center, and the Fundamental Research Funds for the Central Universities (2021RC12), the Shenzhen Virtual University Park (Szvup010). Shuang Wei, Sheng Liu and Chao Lei contributed equally to this work.

References

[1] G. S. Kanter, D. Reilly, et al., "Practical physical-layer encryption: The marriage of optical noise with traditional cryptography," *IEEE Communications Magazine*, vol. 47, no. 11, pp. 74-81, November 2009.

[2] H. P. Yuen, "KCQ: A New Approach to Quantum Cryptography I. General Principles and Key Generation," https://arXiv:quant-ph/0311061v6, 2003.

[3] M. Yoshida, T. Kan, K. Kasai, et al., "10 Tbit/s QAM Quantum Noise Stream Cipher Coherent Transmission Over 160 Km," *Journal of Lightwave Technology*, vol. 39, no. 4, pp. 1056-1063, 2021.

[4] C. Lei, J. Zhang, Y. Li, Y. Zhao, K. Wang, S. Liu, B. Wang, H. Gao, J. Li, "16 QAM Quantum Noise Stream Cipher Coherent Transmission Over 300 km Without Intermediate Amplifier," *IEEE Photonics Technology Letters*, vol. 33, no. 18, pp. 1002-1005, 2021.

[5] M. Zhang, Y. Li, H. Song, B. Wang, et al., "Security Analysis of Quantum Noise Stream Cipher under Fast Correlation Attack," *2021 Optical Fiber Communications Conference and Exhibition*, pp. 1-3, 2021.

[6] H. Jiao, T. Pu, J. Zheng, H. Zhou, L. Lu, P. Xiang, et al., "Semi-quantum noise randomized data encryption based on an amplified spontaneous emission light source," *Optics Express*, vol. 26, pp. 11587-11598, 2018.

[7] Y. Chen, H. Jiao, H. Zhou, J. Zheng and T. Pu, "Security Analysis of QAM Quantum-Noise Randomized Cipher System," *IEEE Photonics Journal*, vol. 12, no. 4, pp. 1-14, Aug. 2020, Art no. 7904114,

[8] J. Cho and P. J. Winzer, "Probabilistic Constellation Shaping for Optical Fiber Communications," *Journal of Lightwave Technology*, vol. 37, no. 6, pp. 1590-1607, 2019.