Optics Letters

Implementation of 400 Gbps quantum noise stream cipher encryption for 1520 km fiber transmission using end-to-end deep learning

Yunhao Xie, Xianran Huang, Guozhi Xu, Junzhe Xiao, Mengyue Shi, Weisheng Hu, and Lilin Yi*

State Key Laboratory of Advanced Optical Communication Systems and Networks, School of Electronic Information and Electrical Engineering, Shanghai Jiao Tong University, Shanghai 200240, China
**lilinyi@sjtu.edu.cn*

Received 26 December 2024; revised 13 April 2025; accepted 7 May 2025; posted 8 May 2025; published 2 June 2025

In the era of large models and big data, the security of optical fiber communication backbone networks has garnered significant attention. Quantum noise stream cipher (QNSC) stands as a crucial method for safeguarding the physical layer security of optical fiber communications, yet the current schemes lag behind the rate capabilities of existing 400G optical fiber backbone networks. In this paper, we introduce deep learning into QNSC and propose an end-to-end quantum noise stream cipher (E2E-QNSC) scheme, which encrypts 16 quadrature amplitude modulation (QAM) into E2E-65536QAM/QNSC. Our experiments successfully demonstrate secure optical communication with a single-channel rate of 400 Gbps, a total capacity of 8.4 Tbps, and a transmission distance of 1520 km. Even in the most extreme scenarios, the detection failure probability (DFP) of the scheme remains at an excellent level greater than 0.9999, proving the security of the approach. The experimental results presented herein represent the highest rate–distance product record of QNSC secure transmission systems, to the best of our knowledge.

https://doi.org/10.1364/OL.553692

The widespread adoption of transformative applications such as artificial intelligence, autonomous driving, and the Internet of Things has driven optical fiber communications to increasingly ambitious goals, pushing for longer transmission distances and vastly higher capacities. As a result, the security of information at the physical layer has become a paramount concern, as these systems now face a broad spectrum of sophisticated threats [1]. To address these emerging risks, a variety of encryption techniques have been proposed, including chaotic encryption [2], quantum noise stream cipher (QNSC) [3], and quantum direct communication [4]. Among these, QNSC has garnered significant attention due to its innovative approach of exploiting the inherent quantum noise present in communication systems [5] to effectively mask the transmitted information.

QNSC encryption schemes can generally be classified into three distinct categories: intensity modulation (IM)/QNSC, which offers a simple, cost-effective structure with practical applicability [5–7]; phase modulation (PM)/QNSC, which is especially well-suited for long-distance transmissions due to its robustness [8–10]; and quadrature amplitude modulation (QAM)/QNSC, which provides an optimal balance of high security, speed, and performance [3,11,12,13]. IM/QNSC schemes have demonstrated successful operation at rates up to 100 Gbit/s, but their transmission distance is inherently limited to approximately 100 km, primarily due to the constraints of IMDD systems [7]. In contrast, PM/QNSC schemes have proven capable of supporting ultra-long-distance transmission, though their data rates remain relatively modest, typically in the tens of Gbit/s range [14]. QAM/QNSC schemes, which strike an ideal compromise between high data rates and extended transmission distances, have been shown to achieve impressive rates of up to 201.6 Gbit/s over 1200 km of optical fiber [3]. However, a significant performance gap remains when compared to the high-rate demands of current 400G ultra-long-haul all-optical backbone transmission systems [15]. Furthermore, in long-distance, multi-span QAM/QNSC transmissions, the cumulative effects of nonlinearity at each span lead to severe degradation in both transmission distance and overall system performance.

Fortunately, artificial intelligence, particularly deep learning, which is a core technology for 6G, enables end-to-end optimization of communication systems, significantly enhancing performance. End-to-end learning-based techniques, such as autoencoders, have proven effective in mitigating channel nonlinearity [16], addressing imperfections in transceiver hardware [17], and recovering bit streams from corrupted signals [18]. In this work, we integrate deep learning into the QNSC transmission system and propose an end-to-end quantum noise stream cipher (E2E-QNSC) scheme. At the transmitter, the neural network encoder encodes and changes the geometric structure of the original standard QAM constellation diagram to generate a geometrically shaped 16QAM signal, which is then encrypted using QNSC to produce an E2E-65536QAM/QNSC signal. At the receiver, a neural network decoder is employed for decoding. Our experiments demonstrate the successful transmission of 400 Gbit/s GS-65536QAM signals over 1520 km of single-mode

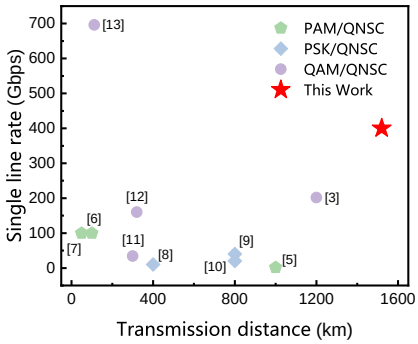

Fig. 1. Transmission distances and single-channel line rates in the previous experimental demonstrations of QNSC.

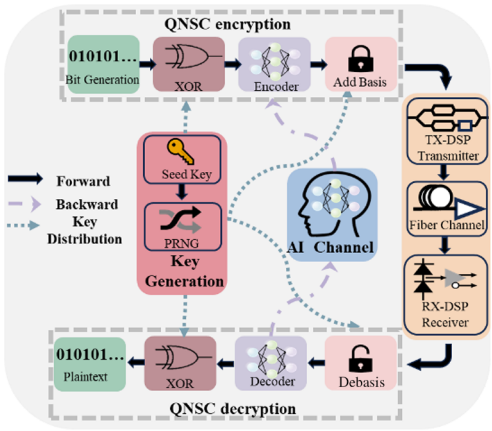

Fig. 2. Principle of the E2E-QNSC.

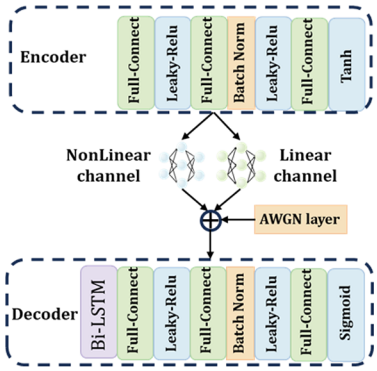

Fig. 3. Structure of the neural network.

fiber with 21-channel wavelength-division multiplexing (WDM) at a 15% soft-decision forward error correction (SD-FEC) threshold (BER = 1.8×10^{-2}). To the best of our knowledge, this represents the highest rate–distance product achieved by QNSC secure transmission systems, as shown in Fig. 1.

The proposed scheme, as illustrated in Fig. 2, shares similarities with traditional QNSC encryption methods [3]. Similar to Ref. [12], the transmitter and the legitimate receiver share a low-speed key seed through key distribution and then use two pseudo-random number generators (PRNGs) to generate two independent high-speed key streams R and B, respectively. These key streams consist of N_S bits and N_B bits, respectively. The key stream R is XORed with the bit information S to enhance security at the bit level, while the other key stream serves as the base state and is added to the mapped constellation points to randomize their positions. The traditional QNSC scheme uses QAM, which is not optimal under different channel conditions (different channel impairments and different device impairments). Therefore, we directly input the encrypted bit stream into the neural network encoder and jointly optimize the constellation point position and binary labeling to achieve the best communication performance [16,17]. The encrypted signal, denoted as S_{QNSC}, can be described as follows:

$$S_{QNSC} = D + B = map(S \oplus R) + B, \quad \textbf{(1)}$$

where map is the constellation mapping rule generated by the neural network encoder. Given the minute interval between adjacent signal levels, which is further obscured by the inevitable presence of quantum noise, an eavesdropper would be prone to making erroneous symbol-level decisions, rendering the extraction of accurate ciphertext infeasible. At the receiver side, the received ciphertext can be expressed as $S_{QNSC} + N$, where N represents the influence of the quantum noise and other residual noise. The legitimate user can perform digital signal processing (DSP) to compensate for channel impairments and use the key to easily subtract the offset to obtain $\hat{D} = \mathrm{S} \oplus R + \mathrm{N}$, where S represents the original signal and N represents the noise. Since the transmitter changes the position of the constellation points, its decision area is irregular. At the same time, there is some residual noise (such as nonlinearity) after passing through DSP. Therefore, we use a neural network decoder for decoding at the receiver. A sliding window of fixed length 2 L + 1 is employed to input the symbol sequence $[\hat{D}(i-L), \cdots, \hat{D}(i), \cdots \hat{D}(i+L)]$ into the decoder. This process allows for the recovery of bit information $\hat{S} \oplus \mathrm{R}$ from the noisy signal. Furthermore, a neural network is utilized to create a digital twin of the optical fiber channel, serving as a differentiable channel for end-to-end training with gradient backpropagation [19]. The objective of training the encoder and decoder is to minimize a combined loss function:

$$\text{loss} = \frac{1}{C}\sum_i (\hat{D}_i - D_i)^2 + \frac{1}{M}\sum_m ((\hat{S} \oplus R)_m - (S \oplus R)_m)^2. \quad \textbf{(2)}$$

Figure 3 illustrates the neural network architecture used in our study, which includes an encoder, a decoder, and a differentiable channel model. The encoder is a multi-layer perceptron (MLP) consisting of three fully connected layers, with leaky ReLU as the activation function. The final layer uses the tanh function to normalize the output to the range [-1,1], facilitating QNSC encryption. The decoder follows a similar structure, combining an MLP with a bidirectional long short-term memory (Bi-LSTM) network. The Bi-LSTM captures dependencies between adjacent symbols, helping mitigate the impact of previous and future symbols on the current symbol's decision. The MLP is designed to recover bit information from noisy symbols as accurately as possible. The final layer applies a sigmoid activation function, normalizing the symbols to the range of 0 to 1. Symbols with soft bit values greater than 0.5 are assigned a value of "1" through hard decision, while values below 0.5 are assigned as "0." For the differentiable channel model that connects the encoder and decoder, we employ the methodology outlined in Ref. [20], wherein a linear model is utilized to learn the linear impairments inherent to the communication channel, while a nonlinear model is designed to capture the

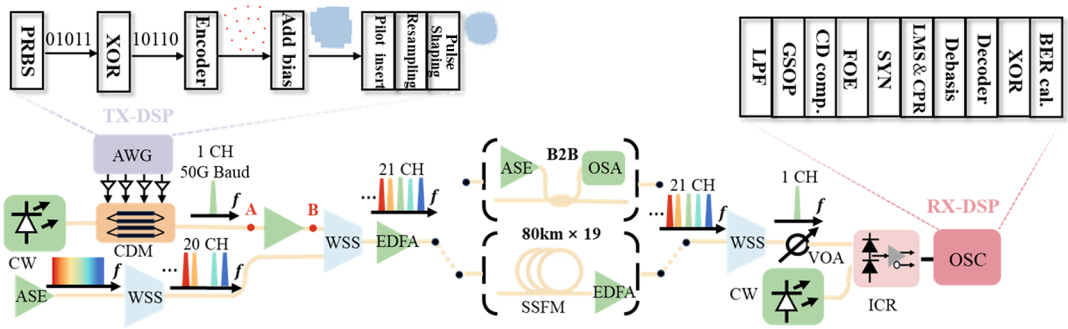

Fig. 4. Experimental setup for 21-channel (400 Gbps per channel) WDM E2E-QNSC transmission over 1520 km.

nonlinear distortion effects present therein. The Gaussian noise, characterized by a normal distribution, undergoes amplitude modulation via a linear layer to emulate the additive white Gaussian noise (AWGN) encountered in practical channels. These three distinct effects—linear impairments, nonlinear distortions, and AWGN—are synergistically superimposed to construct a comprehensive digital twin representation of the actual fiber-optic channel. In actual deployment, the encoder and AI channel will not be used all the time. The rules generated by the encoder will only replace the traditional QAM, and the receiver will use the decoder for decoding. Therefore, it will only cause a delay of tens of microseconds and will not have other negative effects [21]. At the same time, if the E2E-QNSC scheme is to be generalized to multiple scenarios, we can input the channel conditions into the neural network for training as in Ref. [22].

The experimental setup for GS-QNSC is shown in Fig. 4. At the transmitting end, the legitimate user generates an encrypted E2E-65536QAM/QNSC signal using the method described above. The 50G baud dual-polarization signal is then sent to a 120 GSa/s arbitrary waveform generator (AWG, Keysight M8194A). Light with a linewidth of 100 kHz at 1550 nm, generated by a continuous-wave laser (CW), is injected into a coherent driver modulator (CDM) with a 3 dB bandwidth of 40 GHz. Limited by experimental conditions and bandwidth constraints, we use a wavelength selective switch (WSS) with a channel spacing of 75 GHz to create a 21-channel WDM transmission system, in which one channel is used as the channel under test (CUT) and the remaining 20 channels are filled with amplified spontaneous emission (ASE) noise. In the transmission link, the signal travels through 19 spans, totaling 1520 km in length. After each span, an erbium-doped fiber amplifier (EDFA) is used to compensate for fiber loss. Additionally, a WSS is placed every eight spans to filter out-of-band noise. After fiber transmission, the signal's power is controlled using a variable optical attenuator (VOA), and a WSS filters out the CUT for demultiplexing. At the receiver, the received optical signal is converted into four electrical signals by an integrated coherent receiver (ICR), while a second CW with a linewidth of 100 kHz serves as the local oscillator (OSC).

The received digital signals are processed using the pilot-based modulation format-independent DSP method proposed in our previous work [23]. The header of the data frame is a pilot sequence of 1024 symbols, which is used for data synchronization and pre-convergence equalizer. Then, a pilot symbol is inserted every 16 symbols to update the equalizer and compensate for phase noise. We insert a single-tone signal in the frequency domain of the data and obtain the frequency offset of the data by the change in the position of the single-tone signal before and after transmission. The equalizer adopts a DD-LMS structure, and the taps are only updated at the pilot symbol, not on the encrypted data. After equalization, the V–V algorithm is used to compensate for the residual noise.

Beforeinitiating end-to-end training within the experimental setup, we conducted a preliminary pre-training phase for the encoder, decoder, and differentiable channel model in a simulated environment, employing the Adam optimizer configured with a learning rate of 1×10^{-3} and a batch size of 512, executed on an NVIDIA GeForce RTX 3090 GPU; the pre-training procedure was structured into two distinct stages: initially, the encoder and decoder underwent 200 epochs of training utilizing conventional rectangular 16QAM signals coupled with Gray coding to expedite model convergence and enhance communication efficacy, and subsequently, an additional 2000 epochs of end-to-end training were executed in a 400 Gbps signal context employing a 1520 km split-step Fourier method (SSFM)-based fiber channel to validate the initial training's applicability and robustness within the experimental framework; following the completion of pre-training, the model was subjected to a fine-tuning process in the experimental environment spanning 500 epochs with the objective of attaining peak performance metrics.

Figures 5(a), 5(b) illustrate the transmission performance of the E2E-QNSC scheme and the conventional QNSC scheme over 1520 km of optical fiber, as well as in a back-to-back (B2B) configuration. Figure 5(a) demonstrates that the optimal launch power for the conventional QNSC scheme is approximately 0.5 dBm. When the launch power exceeds this value, the bit error rate (BER) increases sharply due to fiber nonlinearity. In contrast, the E2E-QNSC scheme allows for a significantly higher optimal launch power of about 1 dBm. This is attributed to the geometric shaping applied by the encoder, which mitigates nonlinear signal impairments, while the receiver-side decoder shows enhanced tolerance to both nonlinear noise and residual linear noise from DSP. Figure 5(b) shows that, at a 7% high-density forward error correction (HD-FEC) threshold, E2E-QNSC provides a 0.98 dB improvement in the optical signal-to-noise ratio (OSNR) compared to the conventional QNSC scheme.

In order to evaluate the security of our scheme, we test the false detection probability (DFP) of the eavesdropper in the experiment. There are two weakest points in the system, Point A and Point B. We elected to test the security at Point B rather than Point A, as while Point A experiences relatively lower impact from ASE noise, the maximum received power at Point A for an eavesdropper is only −10 dBm. In contrast, despite being affected by ASE noise, Point B

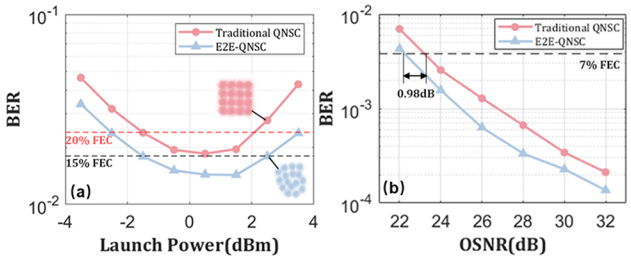

Fig. 5. Experimental results at the rate of 400 Gbps (a) BER versus launch power after 1520 km transmission and (b) BER versus OSNR in the B2B scenario.

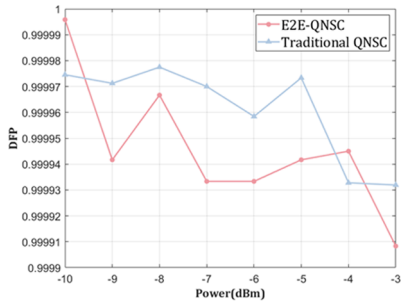

Fig. 6. DFP versus received power at Point B.

offers a higher received power, leading to smaller values of DFP.

Figure 6 shows the variation of DFP with received power. Obviously, as the received power increases, the DFP shows a fluctuating downward trend. However, even at a received power of −2 dBm, the DFP of E2E-QNSC is 0.999908, and that of traditional QNSC is 0.999931, both greater than 0.9999, and there is no significant numerical difference between the two schemes. If an eavesdropper attempts to intercept the signal in the middle of the transmission link, they will encounter ASE noise from EDFA, which will further increase the DFP. This proves the security of the proposed scheme.

In this paper, we introduced the E2E-QNSC scheme, which enables QNSC-secured optical communication over 1520 km of standard single-mode fiber with 21 channels, each operating at 400 Gbps, yielding a total capacity of 8.4 Tbps. Through analysis using DFP, we demonstrated the robustness of our proposed scheme's security. To the best of our knowledge, the experimental results set a new record for the maximum rate–distance product in QAM/QNSC-secured transmission systems, representing a significant milestone. We believe that the proposed scheme will facilitate the future compatibility of QNSC with current coherent optical communication rates and its eventual deployment in ultra-long-haul all-optical backbone networks.

Funding. National Key Research and Development Program of China (2023YFB2905400); National Natural Science Foundation of China (62025503); Shanghai Jiao Tong University 2030 Initiative.

Disclosures. The authors declare no conflicts of interest.

Data availability. Data underlying the results presented in this paper are not publicly available at this time but may be obtained from the authors upon reasonable request.

REFERENCES

1. M. P. Fok, Z. Wang, Y. Deng, *et al.*, IEEE Trans. Inf. Forensics Secur. **6**, 725 (2011).
2. L. Wang, X. Mao, A. Wang, *et al.*, Opt. Lett. **45**, 4762 (2020).
3. J. Sun, L. Jiang, A. Yi, *et al.*, Opt. Express **31**, 11344 (2023).
4. Z. Qi, Y. Li, Y. Huang, *et al.*, Light: Sci. Appl. **10**, 183 (2021).
5. F. Futami, K. Tanizawa, and K. Kato, J. Lightwave Technol. **38**, 2774 (2020).
6. Q. Yu, Y. Wang, D. Li, *et al.*, IEEE Access **8**, 63585 (2020).
7. Y. Wang, H. Li, M. Cheng, *et al.*, Opt. Express **29**, 5475 (2021).
8. K. Tanizawa and F. Futami, Opt. Express **27**, 1071 (2019).
9. K. Tanizawa and F. Futami, Opt. Express **27**, 25357 (2019).
10. F. Futam, K. Tanizawa, and K. Kato, In *European Conference on Optical Communication (ECOC)*, (2019), pp. 2774–2781.
11. C. Lei, J. Zhang, Y. Li, *et al.*, IEEE Photonics Technol. Lett. **33**, 1002 (2021).
12. X. Chen, K. Tanizawa, P. Winzer, *et al.*, Opt. Express **29**, 5658 (2021).
13. J. Sun, L. Jiang, X. He, *et al.*, In *2024 Asia Communications and Photonics Conference (ACP) and International Conference on Information Photonics and Optical Communications (IPOC)*, (IEEE, 2024), pp. 1–5.
14. K. Tanizawa and F. Futami, Opt. Express **29**, 10451 (2021).
15. D. Zhang, M. Zuo, H. Chen, *et al.*, J. Lightwave Technol. **41**, 3774 (2023).
16. R. T. Jones, T. A. Eriksson, M. P. Yankov, *et al.*, In *European Conference on Optical Communication (ECOC)*, (2018), pp. 1–3.
17. R. T. Jones, M. P. Yankov, and D. Zibar, In *European Conference on Optical Communication (ECOC)*, (2019), pp. 1–4.
18. Y. Zhu, J. Ye, L. Yan, *et al.*, J. Lightwave Technol. **41**, 7192 (2023).
19. R. Zhang, M. Liao, J. Chen, *et al.*, In *IEEE INFOCOM 2023-IEEE Conference on Computer Communications*, (2023), pp. 1–10.
20. J. Shi, Z. Li, J. Jia, *et al.*, J. Lightwave Technol. **41**, 2381 (2023).
21. Pedro J. Freire, Michael Anderson, Bernhard Spinnler, *et al.*, In *2022 European Conference on Optical Communication (ECOC)*, (IEEE, 2022), paper We1C.2.
22. Y. Zhang, M. Zhang, Y. Song, *et al.*, J. Opt. Commun. Networking **15**, 985 (2023).
23. Y. Xie, Z. Yang, M. Shi, *et al.*, Adv. Photonics Nexus **3**, 016003 (2024).