hv photonics

IMPACT FACTOR 2.1

CITESCORE 2.6

Article

Analysis of Randomization Capacity in Quantum Noise Randomized Cipher System

Mingrui Zhang, Shuang Wei, Yuang Li, Yajie Li, Yongli Zhao and Jie Zhang

Special Issue

Photonics for Emerging Applications in Communication and Sensing II

Edited by

Dr. Guo-Wei Lu, Prof. Dr. Zhenzhou Cheng and Prof. Dr. Ting-Hui Xiao

MDPI

https://doi.org/10.3390/photonics11111093 *photonics*

MDPI

Article

Analysis of Randomization Capacity in Quantum Noise Randomized Cipher System

Mingrui Zhang, Shuang Wei, Yuang Li, Yajie Li *, Yongli Zhao and Jie Zhang *

State Key Laboratory of Information Photonics and Optical Communications, School of Electronic Engineering, Beijing University of Posts and Telecommunications, Beijing 100876, China
* Correspondence: yajieli@bupt.edu.cn (Y.L.); jie.zhang@bupt.edu.cn (J.Z.); Tel.: +86-139-1106-0930 (J.Z.)

Abstract: We propose and verify a method for analyzing the randomization capacity in a 160 km quantum noise randomized cipher system with different data modulation formats. The randomization capacity is defined as the difference in mutual information between Alice and Bob while the randomization level is at 0 and at its maximum, under the condition of error-free transmission. Our experimental analysis examines the capacity of quantum noise randomized cipher systems under different optical signal-to-noise ratios for each modulation format. Additionally, we analyze the noise masking values while the randomization reaches its capacity. The experimental results indicate that the binary phase shift-keying-based quantum noise randomized cipher system achieves the highest randomization capacity and highest noise masking value.

Keywords: quantum noise randomized cipher; security enhancement; optical fiber communication

check for updates

Citation: Zhang, M.; Wei, S.; Li, Y.; Li, Y.; Zhao, Y.; Zhang, J. Analysis of Randomization Capacity in Quantum Noise Randomized Cipher System. *Photonics* **2024**, *11*, 1093. https://doi.org/10.3390/photonics11111093

Received: 27 October 2024
Revised: 14 November 2024
Accepted: 19 November 2024
Published: 20 November 2024

1. Introduction

Physical-layer security in optical networks is crucial as they face threats that may disrupt services or allow access to confidential data without authorization [1]. The quantum key distribution (QKD) is proposed as a method to stand against these threats [2]. Although QKD can provide unconditional physical-layer security, it suffers from technical imperfections, which pose great challenges to the rates of key generation and transmission distances. QKD has seen breakthroughs in extending secure transmission distances [3] and increasing secret key rates [4]. However, these schemes still require complex equipment to achieve. Compared to QKD, quantum secure direct communication (QSDC) has the advantage of immediacy, as it does not require key establishment before information transmission [5]. Yet, its practical application is limited by the current technological constraints of quantum memory and quantum repeaters. Quantum digital signatures (QDSs) offer a promising approach for the future of digital signatures and data integrity [6,7]. Nevertheless, implementing QDSs requires advanced quantum communication infrastructure, including stable QKD systems and controlled quantum networks. Quantum noise stream cipher (QNSC) is proposed to overcome these challenging implementation difficulties [8–16]. It allows high transmission rates and long distances since the encoding and decoding are performed in digital signal processing (DSP). The security is protected by the quantum noise in the transmission system. Many experiments have been reported for different modulation formats in QNSC, such as phase shift-key (PSK) [8], quadrature amplitude modulation (QAM) [9–12] and intensity modulation (IM) [9–11].

To further enhance the security of QNSC, the technique of quantum noise randomized cipher (QNRC) has been developed. It increases the noise masking by applying randomization in the QNSC symbol. There have been reports of both theoretical and experimental studies related to the QNRC system [14–22]. Recently, the randomization scheme driven by optical temporal scrambling has been proposed [14]. Moreover, applying a chaotic system as a random source is also an effective method to enhance the QNRC [15–19].

All these schemes need a pseudo/true-random number generator as a randomization source for QNRC. Although randomization has shown advantages in enhancing the security of QNRC, existing studies have pointed out that high levels of randomization may significantly decrease transmission performance. Moreover, existing studies have rarely analyzed the limiting capacity of randomization under various conditions. Therefore, it is essential to conduct a quantitative capacity analysis of randomization in QNRC to determine the maximal level of randomization that can ensure both high security and high transmission performance.

In this paper, we propose a capacity analysis method for randomization in QNRC and verify it in 160 km BPSK/QNRC, QPSK/QNRC and 16QAM/QNRC transmission systems. Compared to existing methods, our approach offers unique advantages in analyzing randomization capacity: it enables quantification of system randomization capacity across different modulation formats and optical signal-to-noise ratios, thereby assessing the maximum level of randomization that ensures both high security and transmission performance. Experimental results demonstrate that the BPSK-based 2^M QNRC system has the best capacity performance for randomization. And a higher M leads to a lower capacity. Moreover, BPSK has the highest value of noise masking while the system's randomization level reaches its capacity.

In the following sections, this paper provides a structured analysis of the randomization capacity in QNRC systems. Section 2 introduces the principle of QNRC, explaining the encryption schemes and randomization techniques utilized for different data modulation formats. In Section 3, we present a detailed mathematical framework for calculating randomization capacity across various modulation schemes, including BPSK, QPSK, 16QAM and IM. Section 4 describes the experimental setup used to evaluate QNRC performance over a 160 km optical fiber link and discusses the results, highlighting the security and randomization capacity trade-offs under different conditions. Finally, Section 5 concludes the paper by summarizing key findings and suggesting future directions.

2. Principle of QNRC

Figure 1 shows the DSP module in QNRC at the transmitter and receiver. For QPSK/QNRC and 16QAM/QNRC, the original data stream is firstly mapped into QPSK or 16QAM symbols at the transmitter. Secondly, the randomized signal is encrypted into QAM format with QNRC. In detail, the encrypted QAM is, respectively, generated by 1-bit QPSK or 2-bit 16QAM signal xor M-bit basis (which uses keys generated by pseudo-random number generator (PRNG) and is pre-synchronized by Alice and Bob) in I and Q modes. The encryption rule is also shared by Alice and Bob. The modulation format of such encrypted data is $2^M \times 2^M$ QAM. The mapping rule of QNRC is natural binary mapping instead of gray mapping. Therefore, 2-bit or 4-bit (I + Q) is hidden in one encrypted QAM symbol and the correct decision level of the signal for Eve is covered with quantum noise. Similarly, BPSK or IM symbols can also be encrypted into 2^M BPSK/QNRC or 2^M IM/QNRC symbols. As an example, the constellation of 16 × 16 QAM/QNRC is shown in Figure 1b, where QPSK (1 bit for I and Q, respectively) data are encrypted by using 2×2^3 basis states (3 bits for I and Q, respectively). We use 2-bit information data $S_I = 0$, $S_Q = 1$ and 6-bit basis $B_I = (b_{I3}b_{I2}b_{I1}) = 001$, $B_Q = \left(b_{Q3}b_{Q2}b_{Q1}\right) = 010$ to generate 8-bit encrypted data $E_I = (S_I \oplus b_{I2}b_{I1},\ B_I) = 1001$, $E_Q = \left(S_Q \oplus b_{Q2}b_{Q1},\ B_Q\right) = 1010$. The encrypted binary information E_I and E_Q are converted into decimal constellation levels L_I and L_Q. Then, we apply scrambling to L_I and L_Q as follows: $\left(L_I\prime, L_Q\prime\right) = \left(L_I + i, L_Q + q\right)$, where i and q are randomized perturbations with a standard deviation of γ. Meanwhile, i and q are determined based on random numbers from a random source. Similarly, this disturbance manifests in the phase for BPSK and in the optical intensity for IM. Our previous work demonstrated an integrating key distribution scheme based on the physical layer of optical fibers. The generated keys have been proven to exhibit good randomness, which can be used as a random source for QNRC [23–25]. Finally, training sequences and pilots are inserted into randomized I/Q signals for transmission.

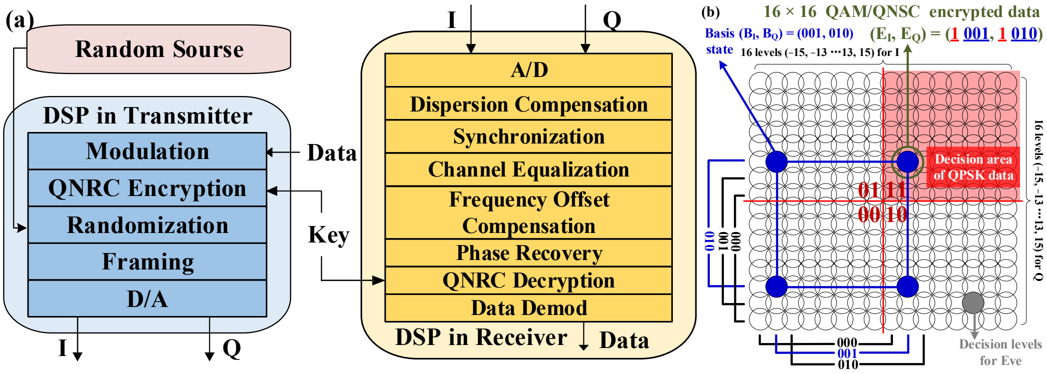

Figure 1. (**a**) DSP in QNRC system. (**b**) Example of QPSK data encrypted into 16 × 16 QAM/QNRC before randomization.

Figure 2 shows the principle of randomization in QNRC for different data modulation. The blue and pink areas represent the noise masking range before and after randomization, respectively. The effect of randomization directly appears as the increase in the noise masking and the decrease in Bob's receiver performance. Nevertheless, Bob can receive the data correctly as long as γ is below a critical level. This fact leads us to the motivation of capacity analysis of randomization.

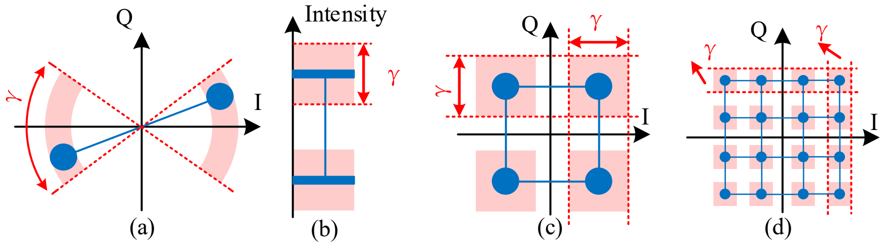

Figure 2. Principle of randomization in QNRC for different data modulation. (**a**) BPSK (**b**) IM (**c**) QPSK (**d**) 16QAM.

3. Randomization Capacity

The capacity of randomization (C_R) is defined as the difference in mutual information between Alice and Bob between $\gamma = 0$ and maximal γ. The value of maximal γ is obtained when the bit error rate (BER) of Bob reaches the forward error correction (FEC) threshold P_{th}. The specific calculation method of mutual information in BPSK and IM (N-level) is shown in Equations (1) and (2).

$$I_0(y;x) = H(y) - H(y|x), \tag{1}$$

$$I_{th}(y;x) = H(y) + P_{th}\log_2 P_{th} + (1-P_{th})\log_2(1-P_{th}), \tag{2}$$

where x is the data from Alice before transmission, y is the data received by Bob. C_R is related to I_0 and I_{th} based on Equations (1) and (2). I_0 represents the mutual information between Alice and Bob without randomization. A higher value of I indicates better system transmission performance, which is influenced by factors such as system noise and optical fiber nonlinearity. Meanwhile, I_{th} represents the mutual information between Alice and Bob with randomization while BER reaches P_{th}. The value of I_{th} depends on P_{th}. It can be observed that the C_R of the system increases as the system transmission performance improves or a more powerful FEC algorithm with a higher threshold P_{th} is employed. C_R for BPSK and IM is as Equation (3) to Equation (5).

$$H(y) = -\sum_{y=0}^{1} P(y)\log_2 P(y), \tag{3}$$

$$H(y|x) = -\sum_{x=0}^{1}\sum_{y=0}^{1} P(x)P(y|x)\log_2 P(y|x), \tag{4}$$

$$C_R = [I_0(y;x) - I_{th}(y;x)]_{P(x)=\frac{1}{N}}, \tag{5}$$

Similarly, the calculation methods of mutual information and C_R in QPSK and 16QAM ($N \times N$-level), are given, respectively, by Equation (6) to Equation (10).

$$I_0(y_I, y_Q; x_I, x_Q) = H(y_I, y_Q) - H(y_I, y_Q|x_I, x_Q), \tag{6}$$

$$I_{th}(y_I, y_Q; x_I, x_Q) = H(y_I, y_Q) + P_{th}^2 \log_2 P_{th}^2 + (1-P_{th})^2 \log_2 (1-P_{th})^2 + 2P_{th}(1-P_{th})\log_2 P_{th}(1-P_{th}), \tag{7}$$

$$H(y_I, y_Q) = -\sum_{y_I=0}^{1}\sum_{y_Q=0}^{1} P(y_I, y_Q)\log_2 P(y_I, y_Q), \tag{8}$$

$$H(y_I, y_Q|x_I, x_Q) = -\sum_{x_I=0}^{1}\sum_{x_Q=0}^{1}\sum_{y_I=0}^{1}\sum_{y_Q=0}^{1} P(x_I, x_Q)P(y_I, y_Q|x_I, x_Q)\log_2 P(y_I, y_Q|x_I, x_Q), \tag{9}$$

$$C_R = \left[I_0(y_I, y_Q; x_I, x_Q) - I_{th}(y_I, y_Q; x_I, x_Q)\right]_{P(x_I, x_Q)=\frac{1}{N^2}}, \tag{10}$$

3.1. C_R in BPSK/QNRC

The principle of QNRC differs when data modulation is varied. Hence, the calculation method of C_R is also different for QNRC in different data modulations. Figure 3 shows the principle of BPSK-based QNRC. Data are encrypted by rotating the phase of BPSK with θ_{basis}. After encryption, the constellation becomes a high-order PSK signal. Subsequently, a truly random phase randomization of θ_R is added to the signal. The range of randomization is γ and it has a maximum value of C_R. The randomization increases in the noise masking. In the receiver, only θ_{basis} is subtracted with the pre-shared key. And the effect of randomization decreases Bob's receiver performance.

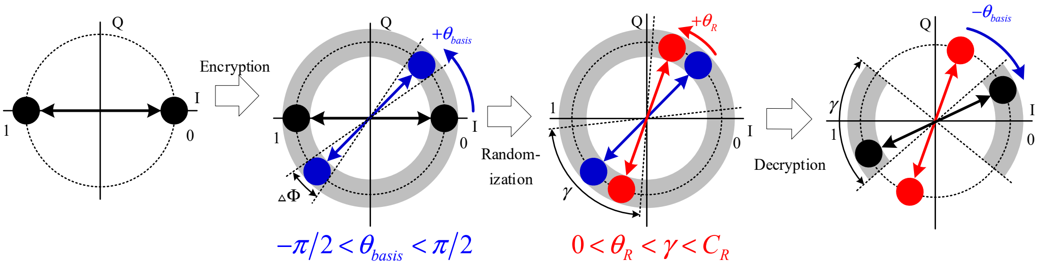

Figure 3. Principle of BPSK-based QNRC.

The noise masking Γ is commonly considered as an evaluation index of security in the QNRC system. In 2^M BPSK/QNRC, the average phase noise $\Delta\overline{\Phi}$ is defined as Equation (11). The Γ_{BPSK} is given as Equation (12).

$$\Delta\overline{\Phi} = \sqrt{\frac{1}{2^M}\sum_{n=1}^{2^M} \Delta\Phi_n^2}, \tag{11}$$

$$\Gamma_{BPSK} = \left(\Delta\overline{\Phi} + \gamma\right)/\Delta\theta, \Delta\theta = \pi/2^{M-1}, \tag{12}$$

The calculation of the bit error ratio for the M-th bit position is as Equation (13). The M-th bit has the lowest bit error rate among 1-st to M-th bits in the 2^M BPSK/QNRC symbol. It is used for data transmission [10].

$$R_{M-BPSK} = \frac{1}{2^{M-1}} \sum_{i=0}^{2^{M-2}-1} \left\{ \frac{1}{2} erfc\left[\frac{\sin\left(i \cdot \pi / 2^{M-1}\right)}{\sqrt{2}\Delta\overline{\Phi}/2} \right] \right\}, \tag{13}$$

Appling $R_{M\text{-}BPSK}$ in Equation (5), C_R in BPSK/QNRC is shown as follows:

$$C_{R-BPSK} = R_{M-BPSK} \log_2 R_{M-BPSK} + (1 - R_{M-BPSK}) \log_2 (1 - R_{M-BPSK}) - P_{th} \log_2 P_{th} - (1 - P_{th}) \log_2 (1 - P_{th}), \tag{14}$$

3.2. C_R in QPSK/QNRC

Figure 4 shows the principle of QPSK-based QNRC. Data are encrypted by translating the amplitude of QPSK with I_{basis} and Q_{basis} in the I/Q channel, respectively. After encryption, the constellation becomes a high-order QAM signal. Subsequently, a truly random amplitude randomization of I_R and Q_R is added to the signal in the I/Q channel. In the receiver, only I_{basis} and Q_{basis} are subtracted with the pre-shared key.

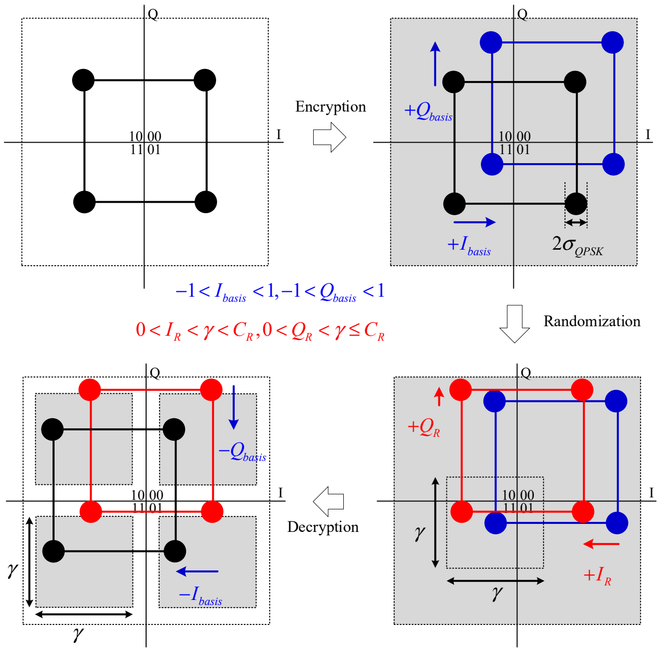

Figure 4. Principle of QPSK-based QNRC.

In QPSK/QNRC, we define the average noise standard deviation $\overline{\sigma}_{QPSK}$ as Equation (15). The Γ for each channel of $2^M \times 2^M$ QPSK/QNRC (I or Q) is given as Equation (16).

$$\overline{\sigma}_{QPSK} = \sqrt{\frac{1}{2 \times 4} \sum_{n=1}^{4} \left(\sigma_{I,n}^2 + \sigma_{Q,n}^2 \right)}, \tag{15}$$

$$\Gamma_{QPSK} = 2\left(\overline{\sigma}_{QPSK} + \gamma\right) / \Delta, \Delta = 2 / \left(2^M - 1\right), \tag{16}$$

The calculation of the bit error ratio for M-th bit position in $2^M \times 2^M$ QPSK/QNRC symbol (I or Q) is as Equation (17) [10].

$$R_{M-QPSK} = \frac{1}{2^{M-1}} \sum_{h=0}^{2^{M-1}-1} \left[\frac{1}{2} erfc \left(\frac{2^M - 1 - 2h}{\sqrt{2}\Gamma_{QPSK}} \right) \right], \tag{17}$$

Hence, in terms of Equation (10), C_R in $2^M \times 2^M$ QPSK/QNRC is shown as follows:

$$\begin{aligned} &C_{R-QPSK} = R_{M-QPSK}^2 \log_2 R_{M-QPSK}^2 + (1 - R_{M-QPSK})^2 \log_2 (1 - R_{M-QPSK})^2 \\ &+2R_{M-QPSK}(1 - R_{M-QPSK}) \log_2 R_{M-QPSK}(1 - R_{M-QPSK}) \\ &-P_{th}^2 \log_2 P_{th}^2 - (1 - P_{th})^2 \log_2 (1 - P_{th})^2 - 2P_{th}(1 - P_{th}) \log_2 P_{th}(1 - P_{th}), \end{aligned} \tag{18}$$

3.3. C_R in 16QAM/QNRC

Figure 5 shows the principle of 16QAM-based QNRC. The operation of encryption, decryption and randomization by translating the amplitude is similar to that of QPSK/QNRC. Yet, the encrypted data represents 16QAM instead of QPSK.

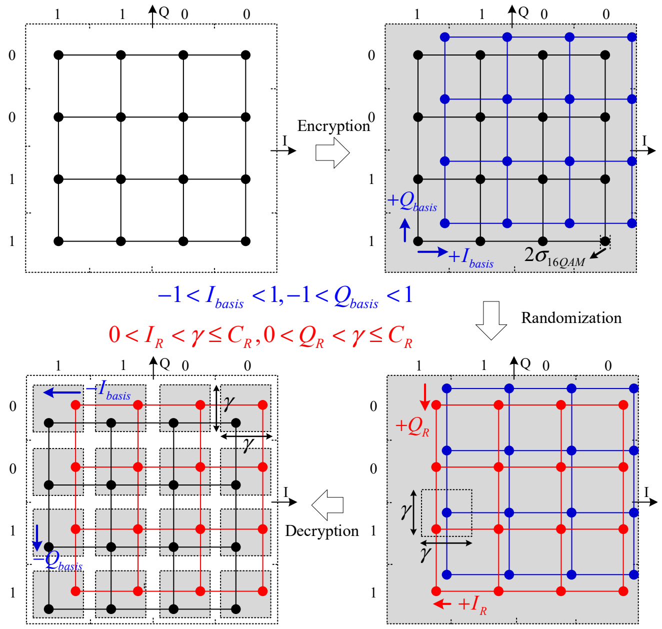

Figure 5. Principle of 16QAM-based QNRC.

Similar to $2^M \times 2^M$ QPSK/QNSC, the average noise standard deviation and Γ in $2^M \times 2^M$ 16QAM/QNRC are as shown in Equations (19) and (20).

$$\overline{\sigma}_{16QAM} = \sqrt{\frac{1}{2 \times 16} \sum_{n=1}^{16} \left(\sigma_{I,n}^2 + \sigma_{Q,n}^2 \right)}, \tag{19}$$

$$\Gamma_{16QAM} = 2(\overline{\sigma}_{16QAM} + \gamma)/\Delta, \Delta = 2/\left(2^M - 1\right), \tag{20}$$

In $2^M \times 2^M$ 16QAM/QNRC, M-th and $M-1$-th bit in each symbol of the I/Q channel is used for data transmission. Their bit error ratios are shown in Equation (21) and Equation (22), respectively.

$$R_{M-16QAM} = \frac{1}{2^{M-1}} \sum_{h=0}^{2^{M-1}-1} \left[\frac{1}{2} erfc\left(\frac{2^M - 1 - 2h}{\sqrt{2}\Gamma_{16QAM}} \right) \right], \tag{21}$$

$$R_{M-1-16QAM} = \frac{1}{2^{M-1}} \sum_{h=0}^{2^{M-2}-1} \left\{ \sum_{j=0}^{1} \left[\sum_{i=1}^{3-2j} (-1)^{i+1} \frac{1}{2} erfc\left(\frac{i2^{M-1}-1-2h}{\sqrt{2}\Gamma_{16QAM}} \right) + \sum_{i=1}^{2j} (-1)^{i+1} \frac{1}{2} erfc\left(\frac{i2^{M-1}-1-2h}{\sqrt{2}\Gamma_{16QAM}} \right) \right] \right\}, \tag{22}$$

While $\overline{R} = (R_{M-16QAM} + R_{M-1-16QAM})/2$, as Equation (10), C_R in $2^M \times 2^M$ 16QAM/QNRC is calculated as follows:

$$\begin{aligned} C_{R-16QAM} = {} & \overline{R}^2 \log_2 \overline{R}^2 + (1-\overline{R})^2 \log_2 (1-\overline{R})^2 + 2\overline{R}(1-\overline{R}) \log_2 \overline{R}(1-\overline{R}) - P_{th}^2 \log_2 P_{th}^2 \\ & -(1-P_{th})^2 \log_2 (1-P_{th})^2 - 2P_{th}(1-P_{th}) \log_2 P_{th}(1-P_{th}), \end{aligned} \tag{23}$$

3.4. C_R in IM/QNRC

Figure 6 shows the principle of IM-based QNRC. Data are encrypted by adjusting the intensity with P_{basis}. After encryption, the constellation becomes a high-order IM signal. Subsequently, a truly random intensity randomization of P_R is added to the signal. In the receiver, only the P_{basis} is subtracted with the pre-shared key.

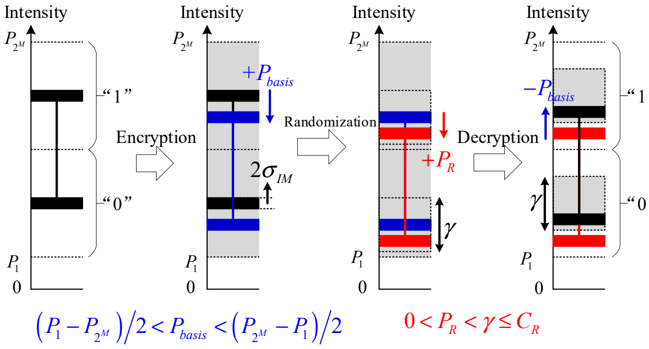

Figure 6. Principle of IM-based QNRC.

The average noise standard deviation and Γ in 2^M IM/QNRC are as shown in Equations (24) and (25).

$$\overline{\sigma}_{IM} = \sqrt{\frac{1}{2^M} \sum_{n=1}^{2^M} \sigma_n^2}, \tag{24}$$

$$\Gamma_{IM} = \frac{(2^M - 1)(r+1)}{r-1} (\overline{\sigma}_{IM} + \gamma), \tag{25}$$

$r = P_{2^M}/P_1$ and P_m is the intensity level of 2^M IM/QNRC ($1 \le m \le 2^M$). The calculation of the bit error ratio for the M-th bit position in the 2^M IM/QNRC symbol is as Equation (26). Hence, as claimed by Equation (5), C_R in 2^M IM/QNRC is shown as Equation (27).

$$R_{M-IM} = \frac{1}{2^{M-1}} \sum_{h=0}^{2^{M-1}-1} \left[\frac{1}{2} erfc\left(\frac{2^M - 1 - 2h}{\sqrt{2}\Gamma_{IM}} \right) \right], \tag{26}$$

$$C_{R-IM} = R_{M-IM} \log_2 R_{M-IM} + (1 - R_{M-IM}) \log_2 (1 - R_{M-IM}) - P_{th} \log_2 P_{th} - (1 - P_{th}) \log_2 (1 - P_{th}), \tag{27}$$

4. Experiment Setup and Results Analysis

Figure 7 shows the experiment setup of 2^M BPSK/QNRC, 2^M IM/QNRC, $2^M \times 2^M$ QPSK/QNRC, and $2^M \times 2^M$ 16QAM/QNRC. At the transmitter, the data are converted by an arbitrary waveform generator (AWG) to an electrical signal at the sampling rate of 10-GSa/s and a digital analog converter (DAC) of 12 bits. An external cavity laser (ECL) sends a beam at 1550 nm with 6 dBm power into an electro-optical converter. For BPSK/QNRC, QPSK/QNRC, and 16QAM/QNRC, the electro-optical conversion is achieved by an I/Q modulator. While an intensity modulator is used in the electro-optical conversion of IM/QNRC. After the variable optical attenuator (VOA), the signal is loaded onto the 160 km (80 km × 2) standard single-mode fiber (SSMF) with an attenuation of 0.2 dB/km.

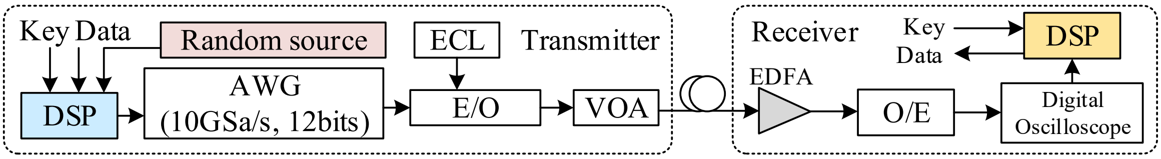

Figure 7. Experiment setup of QNRC.

At the receiver, the received *OSNR* is measured by an optical spectrum analyzer. The received optical signal is amplified into 0 dBm, and then transformed into an electrical signal by an optical-electro converter. For BPSK/QNRC, QPSK/QNRC, and 16QAM/QNRC, the optical-electro conversion is achieved by a coherent receiver which is combined with a local oscillator. While in IM/QNRC, a photoelectric detector is used for optical-electro conversion. The received electrical signals are captured by a digital oscilloscope.

Figure 8a shows the C_R in QNRC (M = 8) with different data modulation for *OSNR* from 1 dB to 25 dB. In our QNRC system with M = 8, higher *OSNR* values lead to higher C_R values. The soft-decision FEC (SD-FEC) with low-density parity-check codes we used has a threshold P_{th} of 4 $\times 10^{-2}$. Consequently, the maximum achievable C_R in our system is 0.242. This value can be further improved by using a more powerful SD-FEC algorithm. However, it will increase the computational complexity of the receiver. For BPSK, QPSK, 16QAM, IM (r = 3) and IM (r = 2) data modulations, the C_R exceeds 0 at *OSNR* values of above 0, 6, 10, 14 and 17 dB, respectively. Moreover, the C_R reaches 0.242 at *OSNR* values of above 7, 13, 17, 21 and 24 dB, respectively. These results suggest that BPSK modulation provides the best capacity performance for randomization compared to other data modulations in the QNRC system with M = 8.

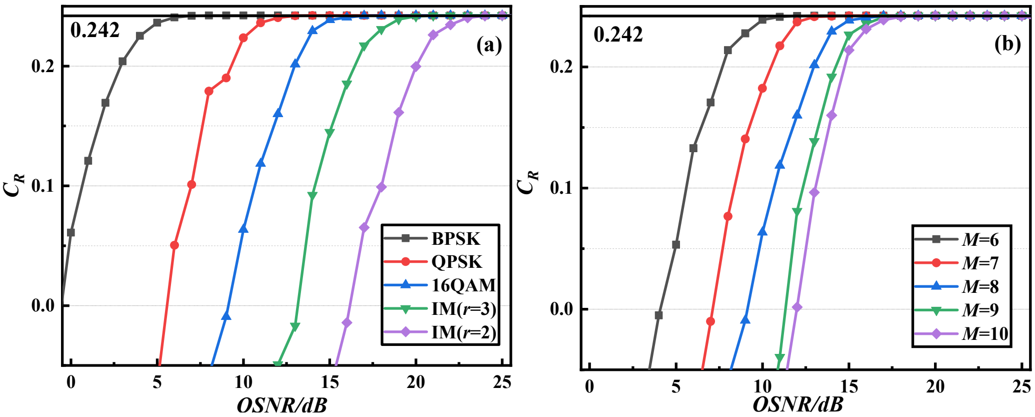

Figure 8. (**a**) C_R for *OSNR* in QNRC (M = 8) with different data modulation. (**b**) C_R of $2^M \times 2^M$ 16QAM/QNRC for various *OSNR*.

Figure 8b illustrates the C_R performance of $2^M \times 2^M$ 16QAM/QNRC for various *OSNR* values. For M = 6, 7, 8, 9 and 10, the C_R exceeds 0 at *OSNR* values of above 5, 8, 10, 12, and 12 dB, respectively. Additionally, the C_R reached 0.242 at *OSNR* values of above 12, 14, 17, 19, and 20 dB for M = 6, 7, 8, 9 and 10, respectively. Meanwhile, C_R increases as the increase in *OSNR* and a higher M leads to a lower C_R value. This result is due to the increased complexity of the QAM modulation scheme at higher values of M, which makes the transmission more susceptible to noise and impairments.

Figure 9a presents the values of Γ for QNRC (M = 8) when the system reaches C_R at different *OSNR* levels. Despite the increase in *OSNR*, the value of Γ remained relatively stable when the system achieved C_R. However, the choice of data modulation scheme has a significant impact on the value of Γ when the system reaches C_R. For instance, we found that Γ was 283.68, 54.76, 48.49, 134.34, and 142.34 for BPSK, IM (r = 2), IM (r = 3), 16QAM and QPSK while $OSNR = 10$ dB, respectively. These findings demonstrate that BPSK has the highest value of Γ when the randomization reaches C_R. It is worth noting that the value of Γ provides a useful metric for evaluating the security of QNRC [9].

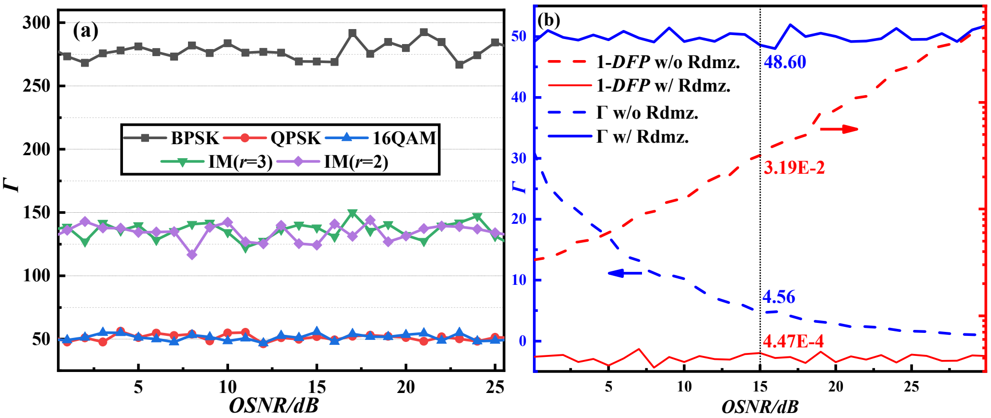

Figure 9. (**a**) Γ for QNRC (M = 8) while the system reaches C_R in different *OSNR*. (**b**) Γ and 1-*DFP* for QPSK/QNRC (M = 8) with or without randomization in different *OSNR*.

Figure 9b shows the Γ and 1-*DFP* for QPSK/QNRC (M = 8) with or without randomization in different *OSNR*. Detection failure probability (*DFP*) refers to the probability that Eve (an eavesdropper) fails to detect the QNRC symbol that is masked by noise. This measure is often used to evaluate the security level of QNRC systems [8–18]. The calculation method for the DFP of QPSK/QNRC is presented in Equation (28).

$$DFP = 1 - \left\{ 1 - \left[\frac{2^M - 1}{2^M} erfc\left(\frac{1}{\sqrt{2\Gamma_{QPSK}}} \right) \right] \right\} \tag{28}$$

It can be observed that the noise masking number, Γ, for QPSK/QNRC decreases as *OSNR* increases. This is due to the fact that high *OSNR* diminishes the effectiveness of noise masking, thereby compromising the security of the system [9,20]. However, the introduction of randomization raises the value of Γ. When the level of randomization reaches the system's tolerance C_R, for *OSNR* is 15 dB, Γ increases from 4.56 to 48.60. Meanwhile, $1 - DFP$ decreases from 3.19×10^{-2} to 4.47×10^{-4}. The results indicate that the introduction of randomization increases the probability of Eve failing to detect the QNRC symbols, thereby enhancing the security of the QNRC system.

5. Conclusions

In this article, we propose a randomization capacity analysis method for QNRC and verify it in 160 km BPSK/QNRC, QPSK/QNRC, 16QAM/QNRC, and IM/QNRC transmission systems. The experimental results demonstrate that the BPSK-based 2^M QNRC system performs best in terms of capacity performance for randomization. Our findings also suggest that higher modulation orders (M) of QNRC lead to lower capacity, highlighting the trade-off between security and randomization capacity. Additionally, we show that BPSK has the highest value of Γ, which indicates that it is the most secure and effective modulation scheme for randomization when the system reaches its capacity limit. However, this randomization method also has certain limitations. For example, as the modulation order increases (such as with a higher M value), the randomization capacity decreases. This is because higher-order modulation formats are more sensitive to noise and system impairments under complex transmission conditions. For future research, further exploration could focus on enhancing QNRC systems with advanced error correction techniques to improve capacity and security in higher-order modulation schemes. Additionally, investigating alternative randomization sources, such as quantum-based random number generators, may provide increased randomness and robustness [26,27].

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

Funding: This work is supported by NSFC Projects (Grant No.: 62021005), the Fundamental Research Funds for the Central Universities, Beijing Natural Science Foundation (4232011) and BUPT Excellent Ph.D. Students Foundation (CX2023228).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Data is contained within the article.

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

References

1. Skorin-Kapov, N.; Furdek, M.; Zsigmond, S.; Wosinska, L. Physical-layer security in evolving optical networks. *IEEE Commun. Mag.* **2016**, *54*, 110–117. [CrossRef]
2. Shor, P.W.; Preskill, J. Simple proof of security of the BB84 quantum key distribution protocol. *Phys. Rev. Lett.* **2000**, *85*, 441–444. [CrossRef] [PubMed]
3. Zhou, L.; Lin, J.; Xie, Y.M.; Lu, Y.S.; Jing, Y.; Yin, H.L.; Yuan, Z. Experimental quantum communication overcomes the rate-loss limit without global phase tracking. *Phys. Rev. Lett.* **2023**, *130*, 250801. [CrossRef]
4. Grünenfelder, F.; Boaron, A.; Resta, G.V.; Perrenoud, M.; Rusca, D.; Barreiro, C.; Houlmann, R.; Sax, R.; Stasi, L.; El-Khoury, S.; et al. Fast single-photon detectors and real-time key distillation enable high secret-key-rate quantum key distribution systems. *Nat. Photonics* **2023**, *17*, 422–426. [CrossRef] [PubMed]
5. Zhang, W.; Ding, D.S.; Sheng, Y.B.; Zhou, L.; Shi, B.S.; Guo, G.C. Quantum secure direct communication with quantum memory. *Phys. Rev. Lett.* **2017**, *118*, 220501. [CrossRef] [PubMed]
6. Yin, H.-L.; Fu, Y.; Li, C.-L.; Weng, C.-X.; Li, B.-H.; Gu, J.; Lu, Y.-S.; Huang, S.; Chen, Z.-B. Experimental quantum secure network with digital signatures and encryption. *Natl. Sci. Rev.* **2023**, *10*, nwac228. [CrossRef]
7. Cao, X.Y.; Li, B.H.; Wang, Y.; Fu, Y.; Yin, H.L.; Chen, Z.B. Experimental quantum e-commerce. *Sci. Adv.* **2024**, *10*, eadk3258. [CrossRef]
8. Yang, X.; Zhang, J.; Li, Y.; Gao, G.; Zhao, Y.; Zhang, H. Single-carrier QAM/QNSC and PSK/QNSC transmission systems with bit-resolution limited DACs. *Opt. Commun.* **2019**, *445*, 29–35. [CrossRef]
9. 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]
10. Zhang, M.; Li, Y.; Song, H.; Zhu, K.; Zhao, Y.; Zhang, J. Security analysis of a QAM modulated quantum noise stream cipher under a correlation attack. *Opt. Express* **2022**, *30*, 40645–40656. [CrossRef]
11. Yang, X.; Zhang, J.; Li, Y.; Zhao, Y.; Gao, G.; Zhang, H. DFTs-OFDM based quantum noise stream cipher system. *Opt. Fiber. Technol.* **2019**, *52*, 101939. [CrossRef]
12. Sun, J.; Jiang, L.; Yi, A.; Feng, J.; Deng, X.; Pan, W.; Bin, L.; 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]
13. 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]

14. Li, Z.; Zhang, Y.; Pang, H.; Luo, Q.; Zhang, X.; Huang, Y.; Tao, Z.; Fan, Y. Security enhancement of quantum noise stream cipher system based on optical temporal scrambling. *Opt. Fiber Technol.* **2023**, *76*, 103245. [CrossRef]
15. Xiao, N.; Shi, S.; Ouyang, H.; Yang, H. Physical-layer security analysis of a quantum noise randomized cipher assisted by chaos masking. *Opt. Fiber Technol.* **2023**, *78*, 103330. [CrossRef]
16. 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.* **2024**, *171*, 110407. [CrossRef]
17. Wang, B.; Li, Y.; Lei, C.; Zhao, Y.; Zhang, J.; Wang, X. Quantum noise diffusion mapping based on chaotic recurrent neural network in quantum noise cipher. In Proceedings of the Asia Communications and Photonics Conference, Beijing, China, 24–27 October 2020; p. M4A.214.
18. Wang, B.; Li, Y.; Lei, C.; Zhu, K.; Zhao, Y.; Zhang, J. Experimental demonstration of security evaluation via hamming distance in quantum noise stream cipher. In Proceedings of the Asia Communications and Photonics Conference, Shanghai, China, 24–27 October 2021; p. T4A.123.
19. Zhu, H.; Gao, M.; Sha, Y.; Li, Z.; Luo, Q.; Shen, G. Security enhancement of one-dimensional chaotic encryption in the physical layer of OFDM-PON. In Proceedings of the Optoelectronics and Communications Conference, Hongkong, China, 3–7 July 2021; p. JS2A.2.
20. Chen, Y.; Jiao, H.; Zhou, H.; Zheng, J.; Pu, T. Security analysis of QAM quantum-noise randomized cipher system. *IEEE Photonics J.* **2020**, *12*, 1–14. [CrossRef]
21. Jiao, H.; Pu, T.; Zheng, J.; Xiang, P.; Fang, T. Physical-layer security analysis of a quantum-noise randomized cipher based on the wire-tap channel model. *Opt. Express* **2017**, *25*, 10947–10960. [CrossRef]
22. Tan, Y.; Pu, T.; Zhou, H.; Zheng, J.; Su, G. Performance analysis of physical-layer security in ISK quantum-noise randomized cipher based on wiretap channel. *Opt. Commun.* **2020**, *461*, 125151. [CrossRef]
23. Li, Y.; Li, Y.; Zhu, K.; Wei, S.; Zhang, M.; Zhao, Y.; Zhang, J. Integrating key generation and distribution with the quantum noise stream cipher system without compromising the transmission performance. *Opt. Lett.* **2023**, *48*, 6500–6503. [CrossRef]
24. Zhu, K.; Zhang, J.; Li, Y.; Wang, W.; Liu, X.; Zhao, Y. Experimental demonstration of error-free key distribution without an external random source or device over a 300-km optical fiber. *Opt. Lett.* **2022**, *47*, 2570–2573. [CrossRef] [PubMed]
25. Zhu, K.; Li, Y.; Zhang, M.; Li, Y.; Zhao, Y.; Zhang, J. 2.5 Gbps Error-free Physical Layer Key Distribution based on Signal Hiding over 80-km SSMF. In Proceedings of the Optical Fiber Communications Conference, San Diego, CA, USA, 24–28 March 2024; p. M4D.4.
26. Eaton, M.; Hossameldin, A.; Birrittella, R.J.; Alsing, P.M.; Gerry, C.C.; Dong, H.; Cuevas, C. Resolution of 100 photons and quantum generation of unbiased random numbers. *Nat. Photonics* **2023**, *17*, 106–111. [CrossRef]
27. Gehring, T.; Lupo, C.; Kordts, A.; Nikolic, D.S.; Jain, N.; Rydberg, T.; Pedersen, T.B.; Pirandola, S. Homodyne-based quantum random number generator at 2.9 Gbps secure against quantum side-information. *Nat. Commun.* **2021**, *21*, 605. [CrossRef] [PubMed]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.