Statistical Analysis of Amplitude Masking for Quantum Noise Stream Cipher by Intensity Modulation

Zhaoyun Li[1,2], Yugang Huang[1], Xin Zhang[2], Qingsong Luo[2], Xiaodong Liang[2], Yukun Zhang[1], Haiyue Pang[1], Zhiyong Tao[1], and Yaxian Fan[1(✉)]

[1] Key Laboratory of Cognitive Radio and Information Processing, Ministry of Education, Guilin University of Electronic Technology, Guilin 541004, China
yxfan@guet.edu.cn

[2] Guangxi Key Laboratory of Optical Network and Information Security, 34th Research Institute of China Electronics Technology Group Corporation, Guilin 541004, China

Abstract. The statistical characteristics of amplitude masking for quantum noise stream cipher by intensity modulation is investigated, which is a Gaussian decomposition fitting based on the distribution probabilities of QNSC signals. The level amplitude distribution probability and standard deviation of noise of QNSC signal can be estimated, even if the encryption order is greater than 16, the decomposition of the probability density function is very complicated in calculation and produces considerable errors. Ultimate, an analysis of the performance of QNSC signal indicated that with the number of encryption order increasing, the error probability for Eve significantly increase, when the encryption orders are larger than 16, the error probabilities are higher than the hard decision forward error correction threshold 3.8×10^{-3}. On the contrary, the error probability for Bob is always maintained at a relatively low level in this process. It is illustrated that analysis of amplitude statistical characteristics can estimate the security of the QNSC system effectively.

Keywords: quantum noise stream cipher · intensity modulation · Statistical analysis

1 Introduction

A fiber-based communication network is a key infrastructure element for future functions like the fourth industrial revolution aka industry 4.0, the sixth-generation mobile networks abbreviated as 6G, hyperscale data centers and so on. It has the potential to support thousands of applications in the fields of politics, economy and military with speeds and throughput exponentially higher than other networks. However, there are several potential threats of optical signal for the optical fiber communication network, such as fiber bending, optical splitting, evanescent coupling, V groove cut, scattering [1–3].

J. Wang (Ed.): MobiMedia 2023, LNICST 576, pp. 48–56, 2025.
https://doi.org/10.1007/978-3-031-60347-1_5

In the past decades, many scenarios have been proposed to apply in physical-layer secure for optical communication, such as chaotic optical communication (COC) [4–6], optical code division multiple access (OCDMA) [7, 8], optical frequency hopping (OFH) [9–11], optical steganography [12, 13], and quantum noise stream cipher (QNSC) [14–16]. Among them, QNSC is considered to be a promising candidate of security scenario in optical transmission, which is compatible with current and next-generation optical fiber communication. Examples include 10,118-km long-haul transmission with 40 Gbps data rate [17], 10.1 Tbps with online transmitted over 160 km [18], implementing a real-time QNSC channel overlay in four coherent wavelength division multiplexer (WDM) system transmitted over 320 km [19]. The security originates from mapping the data format with low-order modulation to the M-ary signal a with low-order modulation with pre-shared keys, and the quantum noise mask can be added to the M-ary signal to further improve its security. So far, an 4,294,967,296(2^{32})-ary quadrature amplitude modulation (QAM) ciphertext symbol based QNSC system has been realized with a 160Gbps signal transmitted over 320 km [20]. To our knowledge, various eavesdropping strategies have appeared in security analysis for the QNSC system, such as ciphertext-only attacks [21], fast correlation [22] and known-plaintext attacks [23]. However, the security of QNSC has seldom been analyzed by statistical characteristics.

Here, we investigate the statistical characteristics of amplitude masking employed as the security performance metric for QNSC by intensity modulation, and propose a method of Gaussian decomposition fitting based on the distribution probability density data of QNSC. An analysis of the performance of QNSC signal when varying its encryption order, and then the probability density of the signal distribution is decomposed by a series of Gaussian functions. Thereby inverting the basic parameters of different multi-level signals such as level amplitude and distribution probability, standard deviation of noise is used to evaluate the encryption efficiency of the QNSC system.

2 Operating Principle

The based on QNSC by intensity modulation is depicted in Fig. 1. This system consists of an encoder, which is used to implement multi-level code and encrypt optical signal, and a decoder, which generates real time discrimination code and decrypt the ciphertext. Alice sends binary message sequence $\{x_i\}$ to Bob via the fiber channel which called main channel, and the QNSC signal which is a multi-level signal masked by quantum noise is generated by encoder. Specifically, the running keystream $\{k_i\}$ can make the multi-level signal randomly. Meanwhile, Bob receives the QNSC signal called ciphertext and needs to distinguish not multi-level signal but binary signals with the discrimination code which is generated by matched decoder with synchronized running key $\{k_i\}$ using same stream as Alice. On the other hand, Eve can also intercept the QNSC signals from Alice by wiretap channel. However, he must distinguish the multi-level signal with masked by quantum noise in case of knowing no information about the share key. In fact, he cannot distinguish the signals without error due to the disturbance of quantum noise, even if he has the same decoder as Bob.

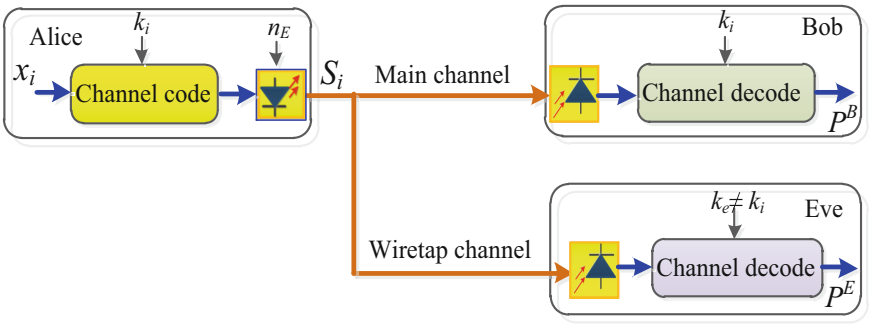

Fig. 1. Statistical analysis model of quantum noise stream cipher.

With reference to the quantum M-ary cipher scheme, the message bit x_i is chopped M-ary string s(k_i,x_i) by keystream k_i bit by bit, it can be expressed by

$$s(k_i, x_i) = s_{min} + k_i \delta s + [(k_i + x_i) \bmod 2] M \delta s + n_E, \tag{1}$$

where, $x_i \in \{0,1\}$ is the binary signal of OOK modulation, $k_i \in \{0,1,\ldots,M\text{-}1\}$ is the keystream, S_{min} is the minimum level for QNSC signal, δs is the intensity difference of adjacent levels, M is the encryption order, $1 \le i \le M$. In the fact, the probability density function $P(S|n_E)$ of quantum noise n_E obeys Gaussian distribution, that is

$$P(S|n_E) \sim \frac{1}{\sqrt{2\pi}\sigma} \exp\left\{-\frac{(S-0)^2}{2\sigma^2}\right\}, \tag{2}$$

where σ^2 is the variance of the quantum noise n_E, and the distribution function of the ith signal can be expressed by

$$P(S|s(k_i, x_i)) \sim \frac{1}{\sqrt{2\pi}\sigma_i} \exp\left\{-\frac{(S - s(k_i, x_i))^2}{2\sigma_i^2}\right\}. \tag{3}$$

And then, the statistics amplitude of QNSC signals for some duration can be expressed by

$$P(S) = a_0 + \sum_{i=1}^{M} a_i \exp\left\{-\frac{(S - s(k_i, x_i))^2}{2\sigma_i^2}\right\}. \tag{4}$$

The sets of encoder basis $\{s(k_i, x_i{\equiv}0), s(k_i, x_i{\equiv}1)\}$ are defined in advance, so Bob can detect the QNSC signals $s(k_i, x_i)$ to decode x_i by discriminating between $s(k_i, 0)$ and $s(k_i, 1)$. And the threshold can be expressed as

$$S_{th}^B(k_i) = \frac{s(k_i, x_i \equiv 0) + s(k_i, x_i \equiv 1)}{2}. \tag{5}$$

Due to the presence of noise in main channel, errors may occur during the decision of signals, the error probability for Bob can be expressed by

$$P_B = 1 - \frac{1}{M/2}\sum_{i=1}^{M/2}\left(\int_{-\infty}^{S_{th}^{B}(k_i)} P(S|\mathrm{s}(k_i, x_i \equiv 0))dS + \int_{S_{th}^{B}(k_i)}^{+\infty} P(S|\mathrm{s}(k_i, x_i \equiv 1))dS\right). \tag{6}$$

Because the transmission channel of fiber is open, Eve also can receive QNSC signals $s(k_i,x_i)$ from Alice by wiretapping. But not the same as Bob, Eve does not have the previously deterministic key k_i, so he cannot determine whether x_i is 0 or 1 through $s(k_i,x_i)$. On the contrary, he has to discriminate the original QNSC signal with M-ary levels which are masked by the quantum noise. Unfortunately, Eve cannot distinguish the signals without error due to the seriously noisy version, and the error probability can be expressed by

$$P_E = 1 - \frac{1}{M}\left(\int_{-\infty}^{s_{min}+\delta s/2} P(S|s_{min})dS + \sum_{i=2}^{M-1}\left(\int_{s(k_i,x_i)-\delta s/2}^{s(k_i,x_i)+\delta s/2} P(S|s(k_i,x_i))dS\right) + \int_{s_{max}-\delta s/2}^{+\infty} P(S|s_{max})dS\right), \tag{7}$$

where s_{max} is the maximum level for QNSC signal. From this, it sees that the probability of correct signal can be estimated by the probability density function of signals.

3 Experimental Setup

We present the experimental setup of security analysis for QNSC system utilizing time-domain statistics in Fig. 2.

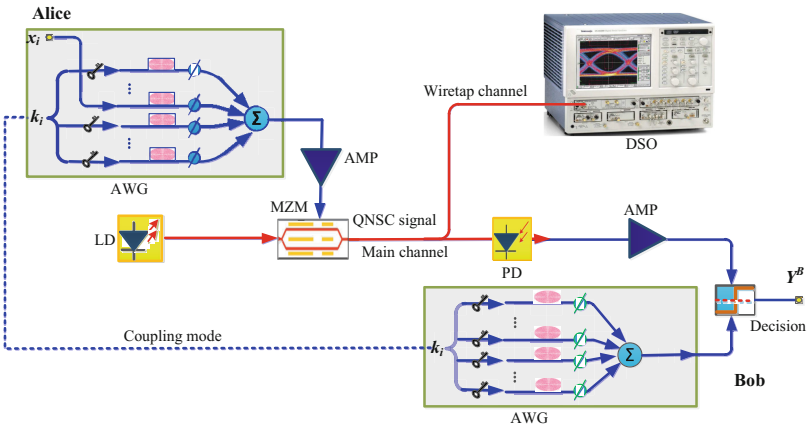

Fig. 2. Experimental setup of security analysis for QNSC system utilizing time-domain statistics. LD: Laser diode, MZM: Mach-Zehnder modulator, PD: Photodetector, AMP: amplifier, AWG: Arbitrary waveform generator, DSO: Digital sampling oscilloscope.

The ONSC signals are generated by an arbitrary waveform generator (AWG, Tektronix AWG70002A) with 10-bit vertical resolution and 10 GS/s sample rate, the corresponding symbol rate can reach 10 Gbaudps. The polarized light output by laser diode

(LD) through polarization maintaining fiber is modulated by the LiNbO3 MZM (Ixblue, MX-LN-10-PD-P-P-FA-FA) driven by the ciphertext symbols from the AWG. When the fluctuation of quantum noise from the laser diode LD masks the adjacent levels of the ciphertext symbols, the QNSC signal is generated. Then, the QNSC signals are captured and sampled by a digital sampling oscilloscope (DSO, Tektronix DSA8200). Additionally, Bob sets an optimal threshold generated by AWG from the second channel with coupling mode to discriminate the x_i since he knows shared k_i. That is, the photodetector (PD) converts the optical signal into M-ary signal masked by noise called IM-QNSC. Then, Bob can recover the signal efficiently by symbol-by-symbol subtraction of the IM-QNSC and the threshold signal which use the same secret keystream as Alice. On the contrary, Eavesdropper must distinguish the M-ary signal from the wiretap channel because of unknowing the secret keystream k_i. Unfortunately, it cannot distinguish the signal due to the noise masking.

4 Results and Discussion

The measured eye diagrams of the QNSC signals are shown in Fig. 3. The encryption order M increased from 2 to 256. In the cases of $M = 2$, the widely opened eye diagram indicates that the binary message sequence $\{x_i\}$ is unencrypted. But the eye diagrams deteriorate rapidly with the encryption order from 2 to 16, even though the eyes are not closed, this is the situation observed in Fig. 3(a)–3(d). When the encryption order M is up to 32 the level spacings much smaller than the noise standard deviation, the eye diagrams completely closed, as shown in Fig. 3(e)–3(f).

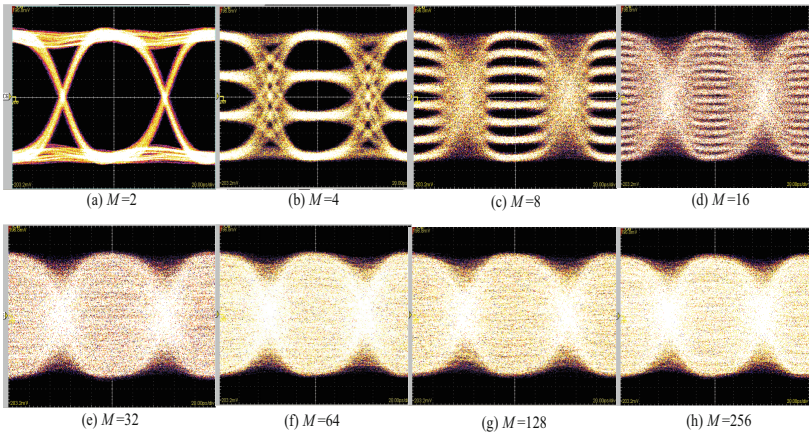

Fig. 3. Eye diagrams of the QNSC signals with different encryption orders.

The histograms of amplitude for QNSC signals are shown in Fig. 4, and the red lines in the figures are the corresponding fit curves. It can be seen from Fig. 4(a)–4(d) that the number of peaks for the amplitude distribution density function correspond to the encryption orders of the signal. With the increase of encryption order, the peak

spacing of the signal distribution probability density function gradually decreases, the peak characteristics have become increasingly difficult to identify, and finally it is completely submerged by noise. It is worth noting that the entire envelope of the amplitude distribution probability density function is similar to a Gaussian function, as shown in Fig. 4(e)–4(h).

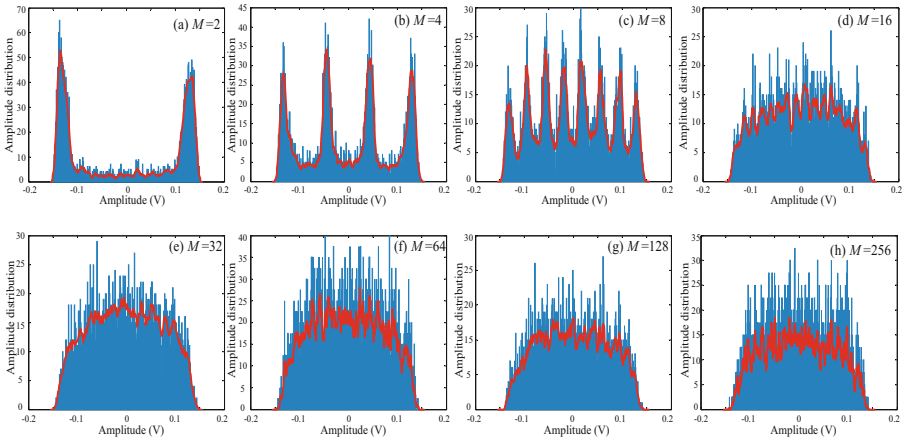

Fig. 4. Histograms of the received QNSC signal samples (blue lines) and corresponding fit curves (red lines). (Color figure online)

This characteristic can be obtained by analyzing the probability density of the hexadecimal signal amplitude distribution shown in Fig. 5, which corresponds to Fig. 3(d).

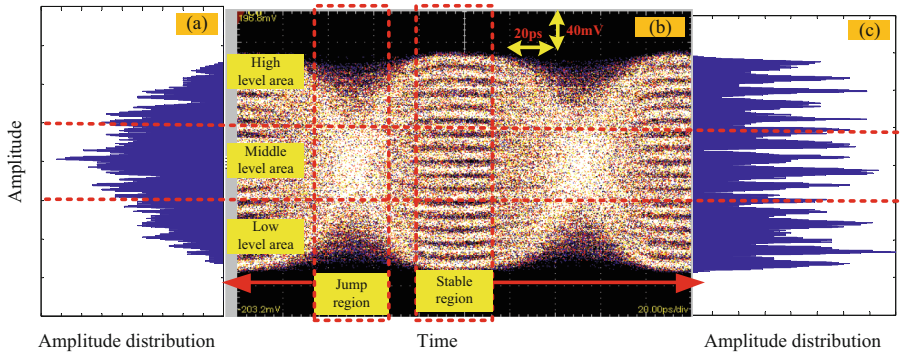

Fig. 5. Amplitude distribution characteristics for QNSC signal.

It can be divided into stable region and jump region in the time axis, and there are three areas which contain high level, middle level and low level, respectively, in amplitude axis, as shown in Fig. 5(b). Here, the signal stable region is shown in Fig. 5(c), the

probability of the occurrence of each level of the multi-level signal is equal, and the amplitude distribution of each signal can be regarded as a uniform distribution function. Meanwhile, the signal jump region is shown in Fig. 5(a), the rising and falling edges of different signal levels overlap less near the high and low levels in the jump process, and the distribution probability is lower, while the distribution probability is higher near the middle level, which is characterized by Gaussian function. The probability density function of amplitude distribution is the superposition of the two regions, so it also follows the Gaussian distribution on the envelope character.

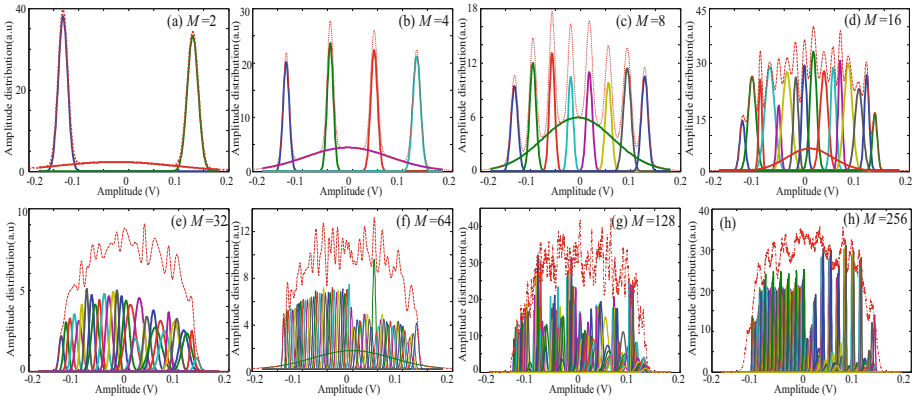

Fig. 6. Decomposition of amplitudes distribution for QNSC signals based on Gaussian function.

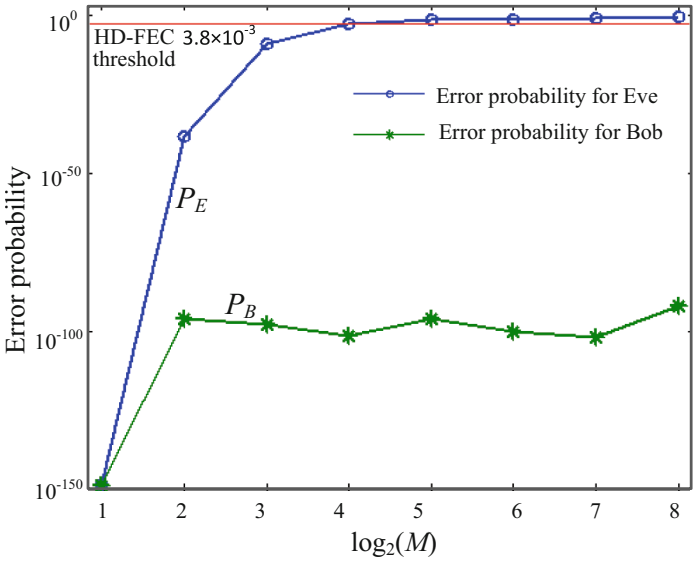

Fig. 7. Error probability between Bob and Eve.

The decomposition of amplitudes distribution for QNSC signals based on Gaussian function are shown in Fig. 6, corresponding to Fig. 4. It can be seen that the lower the encryption order, the easier the amplitude distribution probability density curve is to be decomposed and the better the fitting degree is. As shown in Fig. 6(a)–6(d), when M is greater than 16, the decomposition of the probability density function is very complicated in calculation and produces considerable errors, as shown in Fig. 6(e)–6(h). In spite of this, the basic parameters of different multi-level signals such as level amplitude and distribution probability, standard deviation of noise for QNSC signals can be estimated.

Furthermore, the conditional probabilities of error between Bob and Eve calculated through formula (6) and (7), respectively, are shown in Fig. 7. The curves in Fig. 7 illustrate that with the number of encryption order increasing, the error probability for Eve significantly increase until a stable value close to 0.5, when the encryption orders are larger than 16, the error probabilities are higher than the hard decision forward error correction (HD-FEC) threshold 3.8×10^{-3}, which can ensure the encryption. On the contrary, the error probability for Bob is always maintained at a relatively low level (10–100) in this process. It is indicated that analysis of amplitude statistical characteristics can effectively estimate the security of the QNSC system.

5 Conclusions

In this paper, we investigate the statistical characteristics of quantum noise stream cipher system by intensity modulation by analyzing the eye diagrams with different encryption order. It is shown that with the increasing encryption orders, the signal will be covered by noise, and the eye diagrams of the signal will be closed. Under the condition, the probability density data cannot be well fitted by the Gaussian function. Based on actual estimation, it is indicated that although the assumption of Gaussian density functions still exists a deviation, it can estimate the level amplitude and distribution probability, standard deviation of noise, which can estimate the security characteristics of the QNSC system by comparing error probabilities between Bob and Eve.

Acknowledgement. This research is supported by the Guangxi Natural Science Foundation (Grant No. 2021GXNSFAA220086, 2021GXNSFDA075006), National Natural Science Foundation of China (Grant No. 12064005), and the Guangxi Innovation Driven Development Special Fund Project (Contract No. AB21075009).

References

1. Nina, S.K., Marija, F., Szilard, Z.: Physical-layer security in evolving optical networks. IEEE Commun. Mag. **54**(8), 110–117 (2016)
2. Dahan, D., Mahlab, U.: Security threats and protection procedures for optical networks. IET Optoelectron. **11**(5), 186–200 (2017)
3. Uematsu, T., Hirota, H., Kawano, T.: Design of a temporary optical coupler using fiber bending for traffic monitoring. IEEE Photonics J. **9**, 1–13 (2017)
4. Gao, Z., Wu, Q., Lei, L.: Experimental demonstration of synchronous privacy enhanced chaotic temporal phase en/decryption for high-speed secure optical communication. Opt. Express **30**(17), 31209 (2022)

5. Argyris, A., Syvridis, D., Larger, L.: Chaos-based communications at high bit rates using commercial fiber-optic links. Nature **438**(7066), 343–346 (2005)
6. Shen, L., Wang, Z., Yang, M.: Experimental Demonstration of Chaotic Secure Transmission with Mutual Injection of Semiconductor Lasers over 130-km Multi-Core Fiber. OFC, W4C.5. (2023)
7. Lundqvist, H., Karlsson, G.: Evaluation of soft decoding for optical frequency-hopping channels with beat noise. In: IEEE Global Telecommunications Conference. IEEE (2003)
8. Ban, D., Huang, Q., Chen, Y.: A novel optical frequency-hopping scheme based on a flexible structure for secure optical communications. IEEE Photonics J. **11**(1), 1 (2019)
9. Jin, Y., Qi, Y., Chen, Y.: Secure fiber-optic communication system based on internet-accessible multipath transmission of ciphertext fragments. Opt. Express **29**(16), 24919 (2021)
10. Kodama, T., Nakagawa, N., Kataoka, N.: Secure 2.5Gbit/s, 16-Ary OCDM block-ciphering with XOR using a single multi-port en/decoder. J. Lightwave Technol. **28**(1), 181–187 (2010)
11. Jung, Y., Son, W., Lee, S.: Demonstration of 10 Gbps, all-optical encryption and decryption system utilizing SOA XOR logic gates. Opt. Quant. Electron. **40**(5–6), 425–430 (2008)
12. Wu, B., Tang, Y., Qiu, C.: Secure analysis of optical steganography with spectral signature measurement. IEEE Photonics Technol. Lett. **33**(17), 971–974 (2021)
13. Wohlgemuth, E., Yoffe, Y., Yeminy, T.: Photonic-layer encryption and steganography over IM/DD communication system. Opt. Express **26**(25), 32691–32703 (2018)
14. Barbosa, G., Corndorf, E., Kumar, P.: Secure communication using mesoscopic coherent states. Phys. Rev. Lett. **90**(22), 227901 (2003)
15. Corndorf, E., Liang, C., Kanter, G.: Quantum-noise randomized data encryption for wavelength-division-multiplexed fiber-optic networks. Phys. Rev. A **71**(6), 062326 (2005)
16. Hirota, O., Sohma, M., Fuse, M.: Quantum stream cipher by Yuen 2000 protocol: design and experiment by intensity modulation Scheme. Phys. Rev. A **72**(2), 022335 (2005)
17. Tanizawa, K., Futami, F.: Ultra-long-haul digital coherent PSK Y-00 quantum stream cipher transmission system. Opt. Express **29**(7), 10451–10464 (2021)
18. Yoshida, M., Kan, T., Kasai, K.: 10 Tbit/s QAM quantum noise stream cipher coherent transmission over 160 km. J. Lightwave Technol. **39**(4), 1056–1063 (2021)
19. Futami, F., Guan, K., Gripp, J.: Y-00 quantum stream cipher overlay in a coherent 256-Gbit/s polarization multiplexed 16-QAM WDM system. Opt. Express **25**(26), 33338–33349 (2017)
20. Chen, X., Tanizawa, K., Winzer, P.: Experimental demonstration of 4,294,967,296-QAM Based Y-00 quantum stream cipher carrying 160-Gb/s 16-QAM Signals. Opt. Express **29**(4), 5658–5664 (2021)
21. Hirota, O.: Practical security analysis of a quantum stream cipher by the yuen 2000 protocol. Phys. Rev. A **76**(3), 032307 (2007)
22. Zhang, M., Li, Y., Song, H.: Security analysis of quantum noise stream cipher under fast correlation attack. In: Optical Fiber Communications Conference and Exhibition. IEEE (2021)
23. Hirota, O., Sohma, M., Fuse, M.: Quantum stream cipher by the Yuen 2000 protocol: design and experiment by an intensity-modulation scheme. Phys. Rev. A **72**(2), 022335 (2005)