International Journal of Sensor Networks

ISSN online: 1748-1287 - ISSN print: 1748-1279
https://www.inderscience.com/ijsnet

Security demonstration for the quantum noise-based physical layer using variable keys

Shuai Shi, Ning Xiao

DOI: 10.1504/IJSNET.2022.10049293

Article History:

Received:	30 June 2022
Accepted:	30 June 2022
Published online:	24 January 2023

Security demonstration for the quantum noise-based physical layer using variable keys

Shuai Shi

34th Institute,
China Electronics Technology Group Corporation,
No. 98, Liuhe Road, Guilin, Guangxi, 541004, China
Email: 2008shishuai@163.com

Ning Xiao*

Department of Information Engineering,
Nanning College of Technology,
No. 317, Yanshan Street, Guilin, Guangxi, 541006, China
Email: 693591988@qq.com
*Corresponding author

Abstract: With the continued advancement of science and technology, a large amount of important information is carried by optical fibre networks. Therefore, it is imperative to use secure transmission strategies to protect important information. The Y-00 cipher that employs multi-order modulation to prevent eavesdropping on ciphertext is a practical candidate for providing data protection at the physical layer. The Y-00 cipher combines the mathematical encryption of multilevel signalling and quantum noise to provide high security to fibre communications. This paper proposes a quantum noise-based physical layer secure transmission scheme, combining the Y-00 cipher with time-domain spectral phase encoding (TDSPE). The operation methods of the Y-00 cipher in the data encryption and TDSPE in the key distribution are introduced. Then, the system performance is investigated by transmission experiments. The noise-masking phenomenon is demonstrated and quantified. The probability of the eavesdropper guessing cipher text correctly is evaluated. Last, the proposed secure transmission is achieved at 1 Gbps over a 100.2 km optical fibre link, with an intensity level of 1,024 and a noise masking number of 71. The experimental results prove the effective feasibility and high security.

Keywords: quantum noise-based; variable keys; physical layer; optical fibre link; Y-00 cipher; TDSPE.

Reference to this paper should be made as follows: Shi, S. and Xiao, N. (2023) 'Security demonstration for the quantum noise-based physical layer using variable keys', *Int. J. Sensor Networks*, Vol. 41, No. 1, pp.60–66.

Biographical notes: Shuai Shi is currently a Senior Engineer at 34 Institute of the CETC. In 2013, he obtained his Master's degree from Guilin University of Electronic Science and Technology, China. His research interest is optic communications, high-speed optical time division multiplexing transmission and optical network security. He has presided over the science and technology projects of Guangxi Province and the development of optical transmission equipment.

Ning Xiao is currently an Associate Professor at Nanning Institute of Technology. He obtained his Master's degree from Guilin University of Electronic Science and Technology in 2013. Her research interests include optical network security and mobile communications. She has presided over five science and technology projects and teaching reform projects of Guangxi Province.

1 Introduction

Recently, internet business activities have been increasing. The expanding internet continuously transmits private and confidential information. It is vital to assure the security of data transmissions in the network (Zhou et al., 2020). Although the second or higher layer of the seven-layer network protocol can implement encryption technologies to improve security, as the computer capabilities evolve, there will be decryption risks. This paper proposes the concept of a physical cipher based on quantum encryption. Worldwide research and study of physical-layer encryption strategies have been previously explored (Zhang et al., 2019). Compared to mathematical ciphers, physical ciphers realise higher levels of security.

The Y-00 cipher (Yuen, 2000) is a basic quantum encryption protocol that uses both mathematical and physical cryptography. The transmitted data are protected by masking the signal level with inherent quantum noise. The Y-00 cipher is suitable for high-rate optical fibre communication systems. The Y-00 cipher can be implemented by phase modulation (Corndorf et al., 2005; Jiao et al., 2017a) and intensity modulation (IM) (Shi and Xiao, 2021; Jiao et al., 2019), and quadrature amplitude modulation (Nakazawa et al., 2014). Differences in security features between the traditional cipher and the Y-00 cipher have been analysed and theoretically show that the Y-00 cipher has higher security than the traditional cipher under typical attacks (Hirota, 2007). The eavesdropping channel model is built to analyse the security of the Y-00 cipher (Mihaljevic, 2007), and a general framework is proposed to develop a secure Y-00 instance. Under a specific eavesdropping model, the security capacity of the channel is theoretically deduced. The maximum-security rate of the Y-00 system is proposed to ensure data security (Jiao et al., 2017b). The security of Y-00 ciphers with different modulated styles is theoretically discussed (Kato, 2017). In addition, some experiments of the Y-00 cipher with high-rate and long-distance fibres have been demonstrated (Hirota et al., 2005; Kanter et al., 2009; Futami et al., 2017; Tanizawa and Futami, 2018; Harasawa et al., 2011; Nakazawa et al., 2017, 2019). Almost all experiments of the Y-00 cipher assume that before the encrypted communication starts, the seed key used at the encryptor and decryptor is shared. However, we focus on a secure communication solution that combines the data encryption with the key distribution because our goal is to develop a quantum-noise physical-layer secure communication with a variable key distribution that can achieve a high rate of 1 Gbit/s and a long transmission distance over 100 km.

This article proposes a physical-layer secure transmission scheme using key distribution and data encryption, with confirmation through experimental demonstrations. We analyse the noise mask number, the probability of correctly guessing the ciphertext, and the bit error rate. Then, we evaluate the combined scheme's transport and security performance. Section 2 briefly describes the proposed communication scheme and outlines the concept of IM-based Y-00 cipher and the theory of TDSPE. Section 3 discusses the experimental configuration and results. The integration of high-rate and secure transmissions is also implemented. Section 4 concludes this paper.

2 Operating principles

Figure 1 shows the architecture of the physical-layer secure transmission. The physical-layer transmission includes keys and ciphertexts, which are used to decrypt the required information at the receiver. It is a known fact that a one-time cipher is theoretically very secure for information. Hence, it is necessary to secure encrypted data communication combined with the secure key distribution. Quantum key distribution (Li et al., 2022; Kalra and Poonia, 2019; Beaudry et al., 2013; Lupo et al., 2018; Curty et al., 2014) uses physical phenomena to ensure the security of key swaps in communications, but the swap rate of the keys is low, which cannot meet the high-rate Y-00 quantum noise stream cipher. TDSPE technology is a secure physical-layer transmission method that converts optical signals to noise-like signals (Wang and Wada, 2007; Jiang et al., 2006; Dai et al., 2010). The security of the TDSPE has been proven. The eavesdropper must decrypt the random scrambling for decoding data without a known key. It is unlikely to succeed due to its insufficient fidelity to detect and maintain the sampled signal. Therefore, the Y-00 cipher may cooperate with the TDSPE transmitting key.

2.1 Data encryption of the Y-00 cipher

The Y-00 cipher has the noise masking signal phenomenon by combining military modulation and random noise. As shown in Figure 2(a), there are M bases, and each base comprises two intensity levels denoted as '0' and '1' separately. There is sufficient difference to differentiate the two levels of each base correctly. Due to the quantum noise superimposed on each intensity level, the interval between the adjacent level in two adjacent information bases is very small, and it is impossible to identify the adjacent levels, as shown in Figure 2(b). Figure 2(c) shows the eye diagram. The transmitter sends 'the base of binary data.' Since the data are encrypted with a symmetric key, the legal receiver can interpret the binary symbols represented as the received information base, even with noise.

The brief principle of the Y-00 cipher is shown in Figure 3. The seed key is expanded in a pseudo-random number generator (PRNG) in the encryptor to generate a longer-running key. The exclusive-OR gate scrambles the polarity of the input binary data. Additionally, the base signal is generated after the multi-order signal generator (MOSG) and Mapper. The scrambled binary data are modulated bit-by-bit by the base signal. After external modulation (EM) modulation, the Y-00 cipher is generated. Inevitable noise is superimposed on the Y-00 cipher from the laser diode (LD) and direct detection (DD). Legitimate users use the same PRNG, MOSG, and seed key in the decryption box; hence, it has the same running key. It is unnecessary to resolve adjacent signals for legal decryptors, who have a known correspondence between the base and the data. The appropriate decision threshold translates the original data.

Figure 1 A physical-layer security communication system with the keys and ciphertexts (see online version for colours)

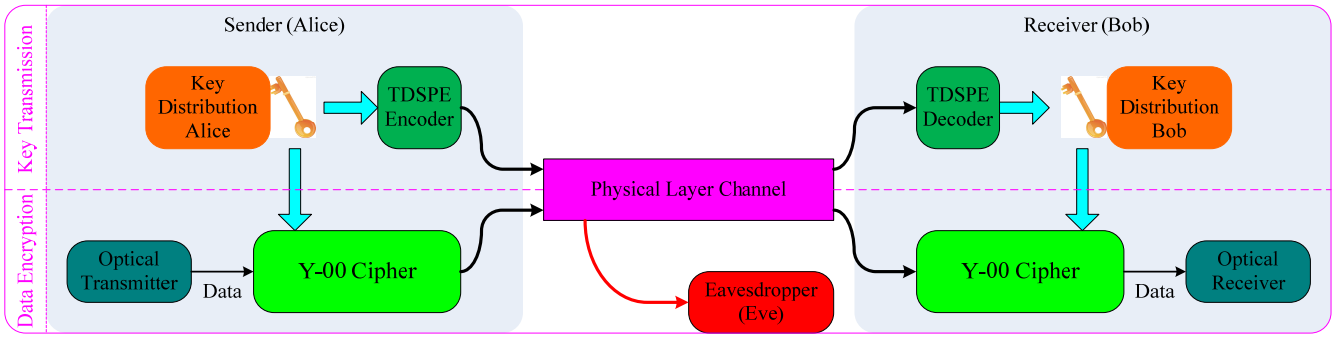


Figure 2 Base concept of the Y-00 cipher (a) set of bases (b) waveform (c) eye diagram

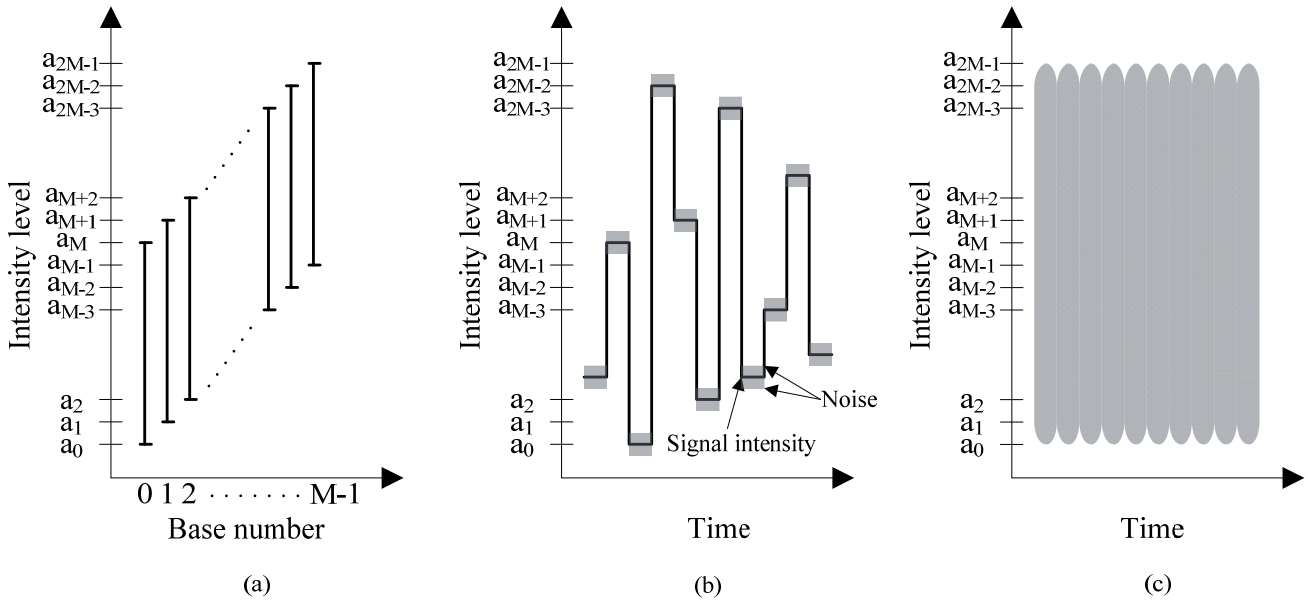


Figure 3 Configuration of the Y-00 cipher

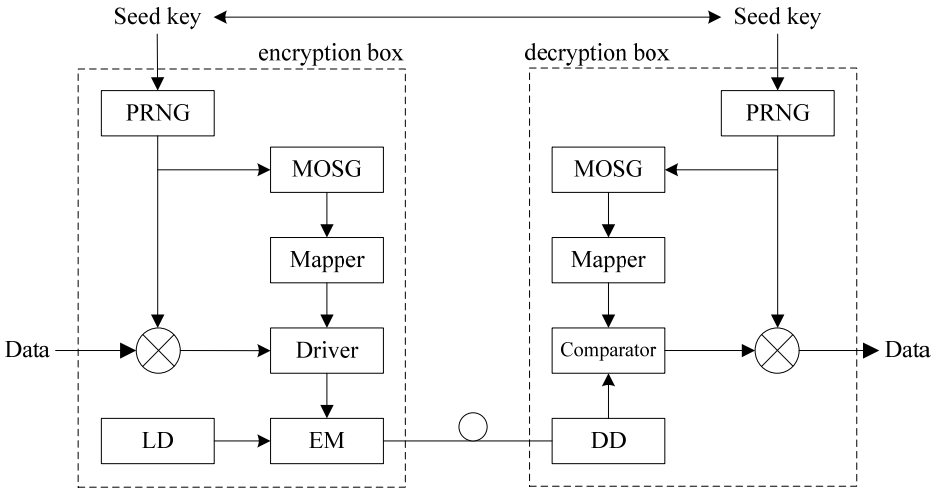
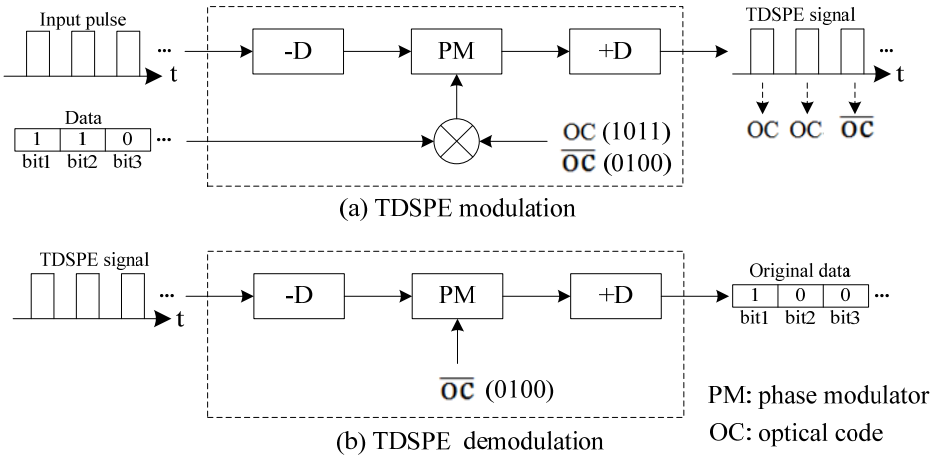


Figure 4 Principle of the TDSPE



2.2 Key transmission of TDSPE

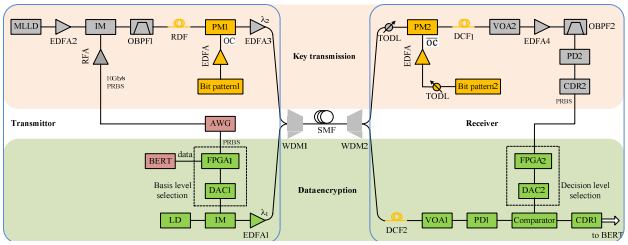
The theory of TDSPE is shown in Figure 4 (Wang et al., 2011). At the transmitter, the ultrashort pulse data are generated by a broad-spectrum laser light source, encoded by TDSPE in the time domain, and then sent to the receiving end. The TDSPE part mainly includes the PM and a pair of dispersion equipment with opposite dispersion values. The -D dispersion device is employed to broaden the pulse data. Then, the OC drives the PM to modulate the stretched pulse. For example, data '1' corresponds to OC, and data '1' corresponds to the complementary OC $(\overline{OC})$. After that, the +D dispersion device compresses the broadened pulse in the time domain to produce the TDSPE signal. At the receiver, the TDSPE signal must be resolved by an appropriate OC first. The configuration is similar to the TDSPE part of the transmitter, including a pair of dispersive equipment and the PM driven only by the $\overline{OC}$. Finally, the original data are restored. We can switch optical codes quickly to improve data confidentiality.

3 Experiments

3.1 Experimental setup

Figure 5 shows a schematic of the experiment. In the transmitter for data encryption, the binary data are generated at 1 Gbps by the BER tester (BERT), and the pseudo-random bit sequence (PRBS) is generated at 10 Gbps by an arbitrary waveform generator (AWG). The base-level selection board converts the serial PRBS into a parallel base. The binary data and base signals form a digital basis level selection signal. The Y-00 cipher signals are generated using a DAC (AD9176, ANALOG DEVICES). The numbers of bases and numbers of optical output signal levels are set to 512 and 1,024, respectively, and the max-to-min power ratio r = 2. A wavelength of λ_1 = 1551.72 nm is set. In the receiver for data decryption, DD implements a photoelectric conversion. A comparator with the delay is used to align the multilevel signal with the decision signal and decrypt the original data. Moreover, a pulse signal is produced by a 10 GHz mode-locked laser diode (MLLD), whose wavelength is λ_2 = 1550.27 nm. Then, a Mach-Zehnder IM modulated by an AWG is utilised at 10 Gbps. The optical bandpass filter (OBPF) has a bandwidth of 2 nm. The dispersion value of the reverse dispersion fibre (RCF) is 405 ps/nm, which causes pulse broadening and overlapping. Afterward, PM1 (ixblue corporation) is driven by OC at 40 Gchip/s. The generated TDSPE signal is sent after amplification by EDFA. The transmission link included the wavelength multiplexer/demultiplexer (WDM) and the 100.2 km single-mode fibre (SMF). The decryptor employs a similar configuration to the encryptor. A DCF with opposite dispersion is applied to compress the pulse. Of course, the dispersion of the SMF link also needs to be compensated. The AWG generates the bit patterns to simplify the experiment. Finally, the CDR outputs the original data after the PD detection and judgment.

Figure 5 Experimental setup (see online version for colours)

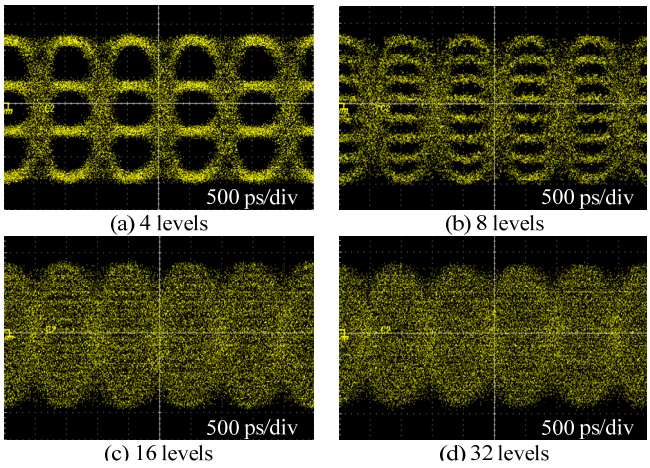


3.2 Experimental results

A 100.2 km ciphertext transmission is demonstrated at 1 Gbps with the security variable key distribution to investigate the proposed scheme. First, we measure the noise-masking phenomenon experimentally. The optical power is set to –17.5 dBm, r is set to 2.0, and the bandwidth of DD is 12.4 GHz. Figure 6 displays eye diagrams of encrypted signals with 4, 8, 16, and 32 levels.

The eyes of the 4-level and 8-level encrypted signals are observed. The eyes of the 16-level and 32-level encrypted signals are completely closed due to noise, even with data processing. It is impossible for an eavesdropper to accurately discriminate between the levels of the multilevel signals to steal the ciphertext that has no shared key, despite observing [Figures 6(c) and 6(d)]. A legitimate user can decrypt the ciphertext correctly due to having the shared key. Therefore, the proposed scheme based on quantum noise encryption can produce effective security. Furthermore, the higher the signal levels, the better the noise masking effect.

Figure 6 Eye diagrams of encrypted signals with 4 levels~32 levels (see online version for colours)



Additionally, we investigate the quantum noise masking signal and its effects on the security and transmission performance. The noise-masking number is a typical security index for quantum-noise stream cipher systems (Shi and Xiao, 2021; Nakazawa et al., 2014). Figure 7(a) depicts the noise masking number, Γ, when the number of signal levels, 2*M*, is changed from 16 to 2048. We assume that the noise intensity of each level is the same because noise crossover means that the noise intensity cannot be measured between multilevel signals (Kato, 2017; Hirota et al., 2005). When the number of bases increases, the noise-mask number gradually increases. Γ is approximately 71 for 2*M* = 1,024 in Figure 7(a). In other words, the noise masks 71 signal levels in the 1,024-level modulation. The system's BER can also be calculated based on the noise-masking phenomenon measured experimentally. Figure 7(b) describes the BER as a function of the number of bases. When the number of bases increases, the BER gradually increases. When the number of bases is not less than 512, the BER is close to 0.5. The decryption process of the quantum stream cipher with 1,024-level IM is similar to the guesswork. This means that the security will be better as the number of bases or levels increases, despite the decrease in transmission performance.

Figure 7 The influence on the performance (a) Noise masking number vs. number of bases (b) BER vs. number of bases

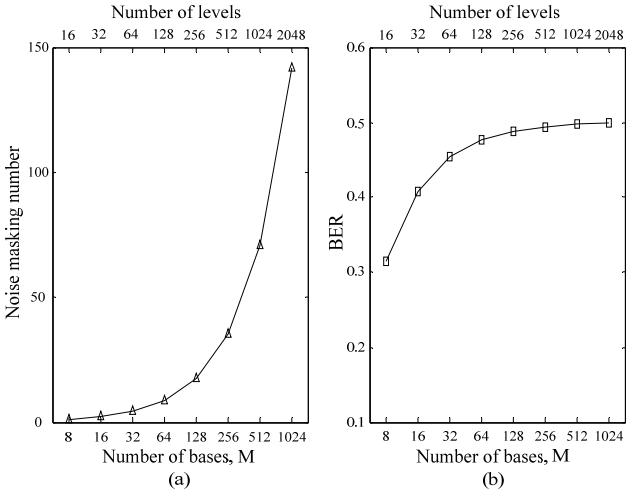


Figure 8 Noise masking number vs. average power (see online version for colours)

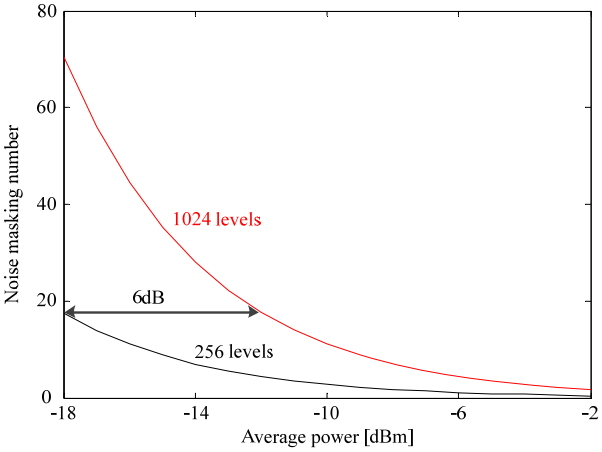


Figure 9 BER vs. average power at the receiver (see online version for colours)

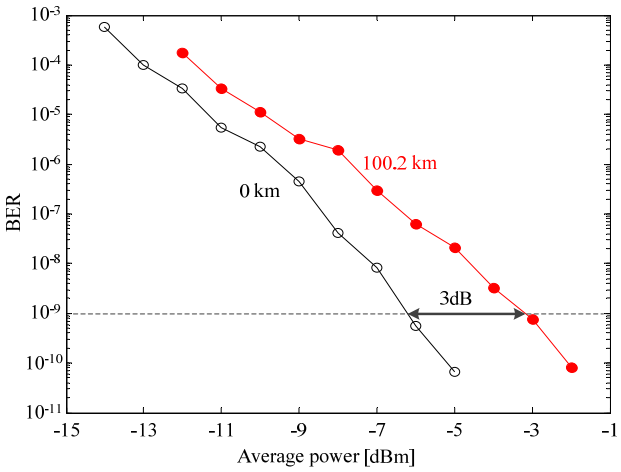
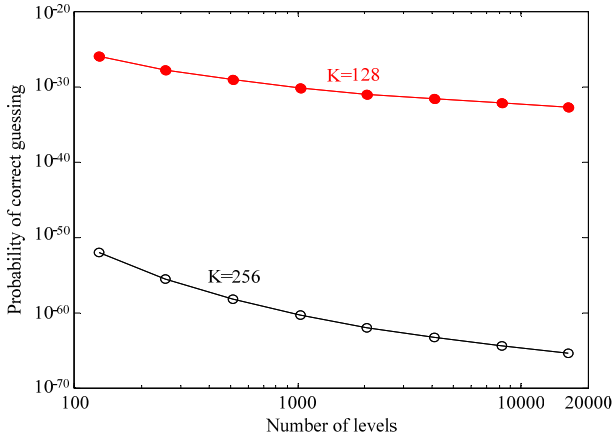
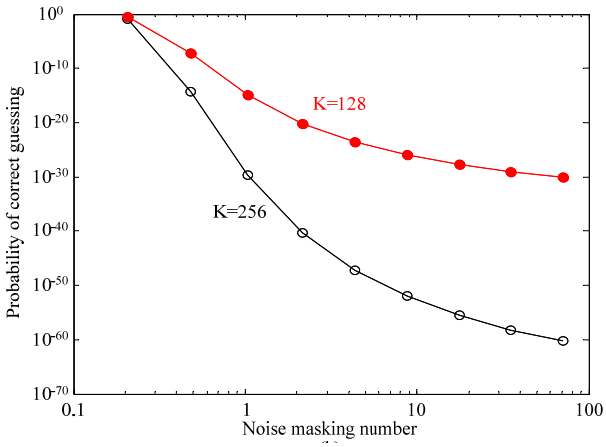


Figure 8 summarises the noise masking number for the average optical power. It decreases as the average optical power increases. The noise-masking number at 1,024 levels is approximately 18 when the average optical power is approximately –12.0 dBm. There is a 6 dB difference in the optical power in the quantum stream cipher with 256 levels and 1,024 levels. Compared with 256 levels for the same noise-masking number, a 6 dB power burden is added to the IM-based quantum stream cipher with 1,024 levels. This indicates that more levels and a lower optical power contribute to better security.

Figure 10 Probability of correctly guessing vs. (a) number of levels (b) noise masking number (see online version for colours)



(a)



(b)

Figure 9 presents the measured BER for $2M$ = 1,024, and the average optical power changes from –14 ~ –2 dBm for a legal recipient (Bob). Error-free transmission (BER ≤ 10^{-9}) can be achieved when the average power is approximately –3.2 dBm after a 100.2 km transmission. In contrast, the average power is reduced to approximately –6.2 dBm for B2B. The power penalty of 3.0 dB between the B2B and the transmissions originates from increased amplifier noise and optical link noise. Additionally, the power penalty becomes small as the max-to-min power ratio increases, decreasing the noise masking number.

It is worth discussing the probability that an eavesdropper can decrypt the ciphertext. We have investigated the detection failure probability of eavesdroppers earlier. Here, we survey the probability that the eavesdropper correctly guesses the ciphertext with the same suppositions as Futami et al. (2018). Figure 10(a) presents the probability of being correct. K denotes the length of the secret key. The probability is 4.9×10^{-61} for $2M$ = 1,024 and K = 256. Next, Figure 10(b) shows that the probability decreases when the noise masking number increases. The probability for Γ = 71 and K = 128 is 6.9×10^{-31}. Additionally, the difference in probability reaches nearly 30 orders of magnitude for K = 128 and K = 256 at $2M$ = 1,024. These results indicate that a higher noise-masking number and more levels benefit better security.

4 Conclusions

We have demonstrated a quantum-noise physical-layer transmission scheme employing the Y-00 cipher and encryption keys transmitted safely by TDSPE. This integration was first proven to provide physical-layer security. In addition, we also introduced the theory of the Y-00 cipher and the phenomenon of noise masking signals. The transmission and security performance of the proposed scheme was investigated experimentally, and the noise masking number and the probability of correctly guessing ciphertext and BER were analysed and assessed. The proposed scheme has proven to have effective feasibility and high security.

Acknowledgements

This research was financially supported by the innovation driven development special fund project of Guangxi Province, PRC (Grant No. 2019AA08002), the project for the basic scientific research ability of young and middle-aged teachers in Guangxi Province, PRC (Grant No. 2020KY58010), and school first-class major in Guangxi Province, PRC (Grant No. ZY202103).

References

Beaudry, N.J., Lucamarini, M., Mancini, S. and. Renner, R. (2013) 'Security of two-way quantum key distribution', *Physical Review A*, Vol. 88, No. 6, p.62302.

Corndorf, E., Liang, C., Kanter, G.S., Kumar, P. and Yuen, H.P. (2005) 'Quantum-noise randomized data encryption for wavelength-division-multiplexed fiber-optic networks', *Physical Review A*, Vol. 71, No. 6, p.62326.

Curty, M., Xu, F., Cui, W., Lim, C.C., Tamaki, K. and Lo, H.K. (2014) 'Finite-key analysis for measure ment-device-independent quantum key distribution', *Nature Communications*, Vol. 5, No. 2, p.3732.

Dai, B., Gao, Z., Wang, X., Kataoka, N. and Wada, N. (2010) 'Demonstration of differential detection on attacking code-shift-keying OCDMA system', *Electronics Letters*, Vol. 46, No. 25, pp.1680–1682.

Futami, F., Guan, K., Gripp, J., Kato, K., Tanizawa, K., Chandrasekhar, S. and Winzer, P.J. (2017) 'Y-00 quantum stream cipher overlay in a coherent 256 Gbit/s polarization multiplexed 16-QAM WDM system', *Optics Express*, Vol. 25, No. 26, pp.33338–33349.

Futami, F., Tanizawa, K., Kato, K. and Hirota, O. (2018) 'Experimental investigation of security parameters of Y-00 quantum stream cipher transceiver with randomization technique: part II', *Proceedings of SPIE*, San Diego, California, USA, p.1077114.

Harasawa, K., Hirota, O., Yamashita, K., Honda, M., Ohhata, K., Akutsu, S., Hosoi, T. and Doi, Y. (2011) 'Quantum encryption communication over a 192-km 2.5-Gbit/s line with optical transceivers employing Yuen-2000 protocol based on intensity modulation', *Journal of Lightwave Technology*, Vol. 29,No. 3, pp.316–323.

Hirota, O. (2007) 'Practical security analysis of a quantum stream cipher by the Yuen 2000 protocol', *Physical Review A*, Vol. 76, No. 3, p.32307.

Hirota, O., Sohma, M., Fuse, M. and Kato, K. (2005) 'Quantum stream cipher by Yuen 2000 protocol: design and experiment by intensity modulation scheme', *Physical Review A*, Vol. 72, No. 2, p.22335.

Jiang, Z., Leaird, D.E. and Weiner, A.M. (2006) 'Experimental investigation of security issues in OCDMA', *Journal of Lightwave Technology*, Vol. 24, No. 11, pp.4228–4234.

Jiao, H., Pu, T., Shi, L., Chen, Y. and Yu, L. (2019) 'A novel realization of quantum stream cipher with key-modulated local light', *Optical Fiber Technology*, Vol. 53, No. 21, p.102007.

Jiao, H., Pu, T., Xiang, P., Zheng, J., Fang, T. and Zhu,H. (2017a) 'Physical-layer security analysis of PSK quantum-noise randomized cipher in optically amplified links', *Quantum Information Process*, Vol. 16, No. 8, p.189.

Jiao, H., Pu, T., Zheng, J. and Su, G. (2017b) 'Physical-layer security analysis of a quantum-noise randomized cipher based on the wire-tap channel model', *Optics Express*, Vol. 25, No. 10, p.10947.

Kalra, M. and Poonia, R.C. (2019) 'Design a new protocol and comparison with B92 protocol for quantum key distribution', *International Journal of Sensor Networks*, Vol. 12, No. 3, pp.153–156.

Kanter, G.S., Reilly, D. and Smith, N. (2009) 'Practical physical-layer encryption: the marriage of optical noise with traditional cryptography', *IEEE Communication Magazine*, Vol. 47, No. 11, pp.74–81.

Kato, K. (2017) 'A unifified analysis of optical signal modulation formats for quantum enigma cipher', *Quantum Communications and Quantum Imaging XV*, *Proceedings of SPIE*, Tokyo, Japan, p.104090K.

Li, X., Zhu, D., Wu, J., Wang, H., Yang, L. and Song, L. (2022) 'A quantum key injection scheme for mobile terminals based on commercial quantum key distribution', *International Journal of Sensor Networks*, Vol. 38, No. 2, pp.132–141.

Lo, H.K., Curty, M. and Tamaki, K. (2014) 'Secure quantum key distribution', *Nature Photonics*, Vol. 8, No. 595, pp.58–67.

Lupo, C., Ottaviani, C., Papanastasiou, P. and Pirandola, S. (2018) 'Continuous-variable measurement-device-independent quantum key distribution: composable security against coherent attacks', *Physical Review A*, Vol. 97, No. 5, p.52327.

Mihaljevic, M.J. (2007) 'Generic framework for the secure Yuen 2000 quantum-encryption protocol employing the wire-tap channel approach', *Physical Review A*, Vol. 75, No. 5, p.52334.

Nakazawa, M., Yoshida, M., Hirooka, T. and Kasai, K. (2014) 'QAM quantum stream cipher using digital coherent optical transmission', *Optics Express*, Vol. 22, No. 4, pp.4098–4107.

Nakazawa, M., Yoshida, M., Hirooka, T., Kasai, K., Hirano, T. and Ichikawa, T. (2017) 'QAM quantum noise stream cipher transmission over 100 km with continuous variable quantum key distribution', *IEEE Journal of Quantum Electronics*, Vol. 53, No. 4, p.8000316.

Shi, S., Xiao, N. (2021) '10-Gsymbol/s IM-based quantum noise encryption system modulated by a dual digital-to-analog converter', *Optical and Quantum Electronics*, Vol. 53, No. 1, p.42.

Tanizawa, K. and Futami, F. (2018) '214 intensity-level 10-Gbaud Y-00 quantum stream cipher enabled by coarse-to-fine modulation', *IEEE Photonics Technology Letters*, Vol. 30, No. 22, pp.1987–1990.

Tanizawa, K. and Futami, F. (2019) 'Single channel 48-Gbit/s DP-PSK Y-00 quantum stream cipher transmission over 400 – and 800-km SSMF', *Optics Express*, Vol. 27, No. 18, pp.25357–25363.

Wang, X. and Wada, N. (2007) 'Spectral phase encoding of ultra-short optical pulse in time domain for OCDMA application', *Optics Express*, Vol. 15, No. 12, p.7319.

Wang, X., Gao, Z., Wang, X., Kataoka, N. and Wada, N. (2011) 'Bit-by-bit optical code scrambling technique for secure optical communication', *Optics Express*, Vol. 19, No. 4, p.3503.

Yuen, H.P. (2000) *A New Quantum Cryptography*, Report in Northwestern University (DARPA Proposed paper).

Zhang, H., Ji, Z., Wang, H. and Wu, W. (2019) 'Survey on quantum information security', *China Communications*, Vol. 16, No. 10, pp.1–36.

Zhou, Y., Charles, M., Wang, T. and Song, M. (2020) 'Improved localisation algorithm based on Markov chain Monte Carlo-metropolis hastings for wireless sensor networks', *International Journal of Sensor Networks*, Vol. 33, No. 3, pp.159–167.