All-digital FPGA-based Real-time 65536-level Quantum Noise Stream Cipher Transmission for Bidirectional CWDM System

Linsheng Zhong[(1)], Ruiyan Zhao[(2)], Yuanxiang Wang[(3)], Hanwen Luo[(1)], Ningchang Zhangsun[(1)], Xiaoxiao Dai[(1)], Mengfan Cheng[(1)], Lei Deng[(1)], Deming Liu[(1)], Bin Zhang[(4)], Zhiwen Fan[(4)], Ping Du[(4)], Liang Mei[(4)], Junbo Xu[(4)], Yaqin Wang[(4)], Qi Yang[(1,2,*)],

[(1)] School of Optical and Electronic Information, Huazhong University of Science and Technology, Wuhan, 430074, China, yangqi@hust.edu.cn

[(2)] Bianfu Optoelec. Technologies Co., Ltd, Wuhan, 430223, China.

[(3)] School of Cyber Science and Engineering, Huazhong University of Science and Technology, Wuhan 430074, China

[(4)] Fiberhome Telecommunication Technologies Co., Ltd., Wuhan 430073, China

Abstract *We demonstrate the first all-digital real-time 65536-level PAM/QNSC transmission based on a typical 4×4 bidirectional CWDM system. The FPGA-based transceivers with CDR function utilize SFP28 optical modules for fiber transmission to achieve protocol-transparent and plug-and-play functionality in existing access network. ©2023 The Author(s)*

Introduction

The importance of communication security has been increasingly emphasized in recent years, as data breaches and cyber-attacks become more prevalent [1]. Quantum Noise Stream Cipher (QNSC) has gained attention due to its superior compatibility with current network framework [2-4]. By mapping the plaintext with low-order modulation format to an ultra-high order ciphertext under the control of key stream, the security comes from masking adjacent ciphertext symbols by inevitable quantum noise. Recently, 10-70 Gbit/s real-time quadrature amplitude modulation (QAM)/QNSC transmission with Field Programmable Gate Arrays (FPGA)-based transmitter and receiver is reported [5-7], showing its potential in achieving high-speed and long-distance communication. However, clock data recovery (CDR) for ultra-high order encrypted signals is a vital problem faced by real-time systems. Existing schemes use an additional link to transmit tone clock signal for optical phase-locked loop (OPLL) [5-7], which restricts the practical feasibility. Moreover, the encryption order highly relies on the resolution of the digital-to-analog converter (DAC). It leads to a limited encryption order, which remains 2^8 in the state-of-art real-time work [6].

In previous work, we proposed DAC/ADC-free and CDR-based QNSC secure system boosted by delta-sigma modulation (DSM). The plaintext capacity up to 4.62 Gbps is demonstrated offline with asynchronous clock [8]. It greatly eases the requirement for high-resolution DAC and clock synchronization. In this paper, we report the first all-digital real-time 65536-level pulse-amplitude modulation (PAM)/QNSC transmission with CDR algorithm. DSM enables delivery and reception of PAM/QNSC signal through off-the-shelf optical modules (OM) without any analog devices. This protocol-transparent and plug-and-play transceiver can be seamlessly connected to the existing network using 10G Small Form-Factor Pluggable (SFP) and 25.78125G SFP28 OMs without any adjustment. The experiment supports bidirectional transmission for 8 users based on CWDM (coarse wavelength division multiplexing) grid to achieve 8×10 Gb/s plaintext capacity. This encryption order of 2^{14} is the highest real-time QNSC result yet reported.

Configuration of FPGA-based real-time transceiver for PAM/QNSC transmission

The FPGA-based real-time transceiver for PAM/QNSC transmission is implemented on the Xilinx Virtex UltraScale+ VU9P platform as shown in Fig. 1. 10-Gbps plaintext is shown in inset(i). The encryption part converts the plaintext

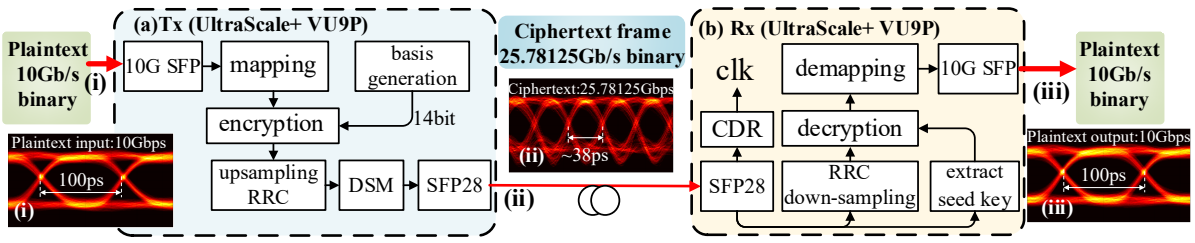

Fig. 1: Configuration of FPGA-based PAM/QNSC real-time transceiver.

into 25.78125-Gbps ciphertext frame (inset (ii)). The rate change here is due to upsampling before DSM. Commercial SFP28 OMs, which are widely deployed in existing fronthaul system [9, 10], are used for transmission. The decryption part completes the reverse process (inset (iii)).

Fig. 1(a) shows a block diagram of the real-time transmitter. After receiving the binary plaintext signal (inset (i)), FPGA maps it to PAM4. Then, the 2-bit sequences are encrypted by modulating their amplitudes with 14-bit basis states generated by 2^{63}-1 pseudorandom binary sequence (PRBS) generators, representing an encryption order of 2^{14}. As a result, 65536-level encrypted signal is generated. The ultra-high order puts high requirements on DACs, leading to high cost and limited ciphertext order. Here, we introduce DSM to convert it into 2-level sequences [11] and replace the amplified spontaneous emission (ASE) noise in the traditional scheme with the quantization noise to mask adjacent ciphertext symbols. To obtain better noise-shaping effect, the PAM/QNSC signal is upsampled by 5 times, and a root raised cosine (RRC) Nyquist filter is adopted. To ensure the randomness and security of the key stream and quantization noise, the seed key located in the header of the frame and DSM parameters are periodically changed at a cycle of 65μs and 1.72s, respectively. The channels of encryption circuit and DSM are 32 and 160 respectively, with the clock of 156.25MHz. Finally, SFP28 OM working at 25.78125Gb/s delivers the framed signal (inset (ii)).

Block diagram of the real-time QNSC receiver is shown in Fig. 1(b). The DSM-PAM/QNSC signals are acquired by SFP28 OMs. In addition, since the transceiver receives low-order digital signals (two-level), the clock signal can be easily extracted through CDR. It eliminates additional clock lines or tone clock signals, which greatly simplifies the system. After RRC, PAM/QNSC signal was decrypted into the original PAM4 data by referring to the extracted seed key parameter. Then, 10-Gbps binary sequence is recovered by the demapper (inset (iii)). Thus, the entire encryption and decryption process is completed without any analog devices.

Fig. 2 depicts the experimental setup for a real-time dual-fiber bidirectional CWDM system assembled PAM/QNSC transceivers. This typical bidirectional system for fronthaul consists of eight CWDM SFP28 OMs with four different wavelengths defined in ITU-T G.694.2 [12], multiplexers (MUX), demultiplexers (DMUX) and two optical fiber cables [13]. The optical spectrum is shown in Fig. 2(i). FPGA-based PAM/QNSC transceivers are connected to a 10G bit error rate tester (BERT). CWDM SFP28 OMs are used to transmit and receive ciphertext. MUX and DMUX enables each fiber to achieve a one-way 4-channel 25 Gbit/s channel capacity. The length of the fiber is 15 km, which is a typical distance for fronthaul applications [14]. Furthermore, the chip planner of the main real-time DSPs (digital signal processing) in FPGA is shown in Fig. 2(c), which can be used to refer to resource consumption.

Results

Histogram of the PAM/QNSC signal without and with decryption is shown in Fig. 3 (a) and (b), respectively. The plaintext (PAM4) is completely

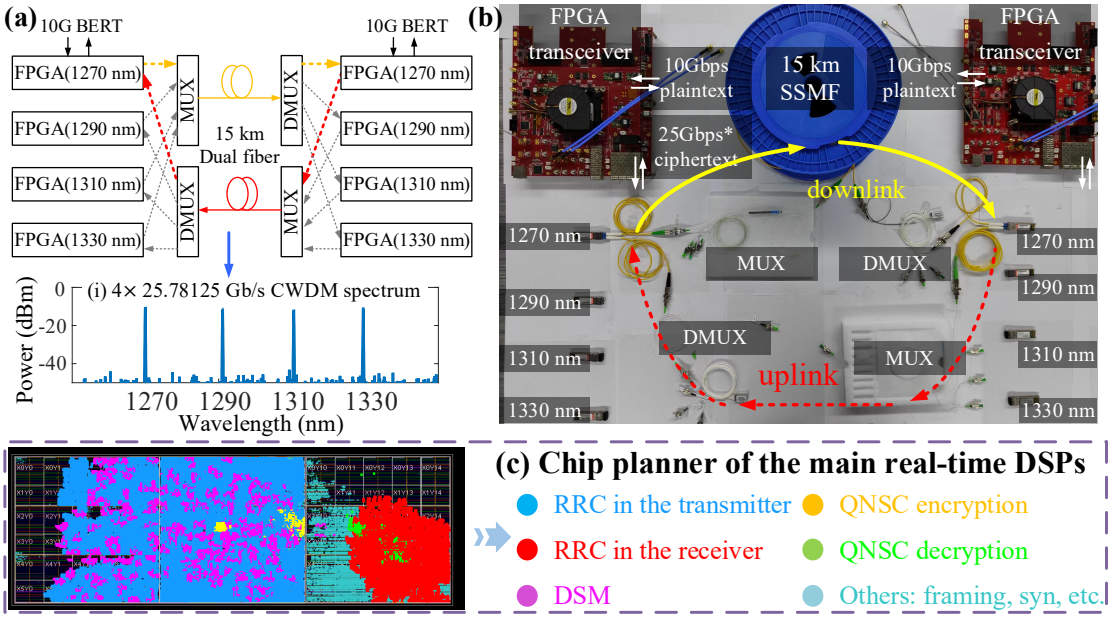

Fig. 2: (a, b) Experimental setup for real-time 4×4 bidirectional CWDM PAM/QNSC system. (c) Chip planner of FPGA.

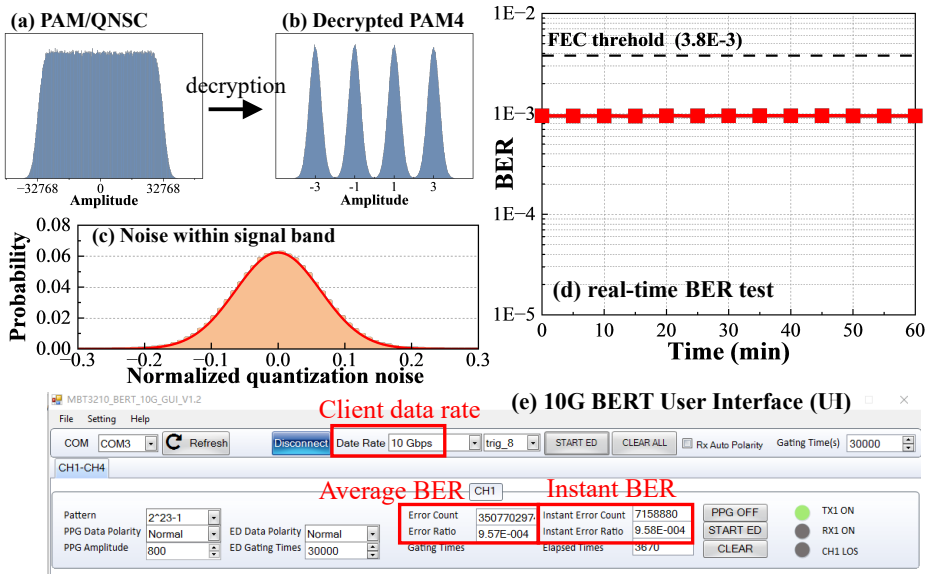

Fig. 3: (a, b) Histograms of PAM/QNSC signal before and after decryption. (c) Distribution of the quantization noise within the signal band. (d) Real-time results with continuous one-hour experiment. (e) BERT User Interface

hidden in a histogram of 65536-level, which is concealed by the quantization noise from DSM. After decryption with the secret keys, original data are recovered as clear PAM4 data as shown in Fig. 3(b). The key seed pattern for encryption are periodically changed at a cycle of 65μs, which greatly enhances system security.

One of the core ideas is to replace quantum noise with quantization noise. Figure 3(c) shows the distribution of the quantization noise within the signal band. To compare with Gaussian white noise, standard fitting curves (red line) of the histogram are provided. We can see that the histogram is basically consistent with the fitting curve, indicating that the quantization noise can be considered as white noise with standard normal distribution. The order and parameters of DSM are the main factors that affect the power and distribution of noise [15]. We also add some random factors to the DSM architecture to increase the randomness of the masking noise for better security performance. One set of parameters includes 6 variables, and the fluctuation cycle is set to 1.72s.

A real-time test result of PAM/QNSC encryption and decryption is shown in Fig. 3(d). Instant and average BER value can be read directly from 10G BERT as shown in Fig. 3(e). After one hour of continuous experiments, results are recorded every five minutes. In the bidirectional CWDM communication system, 10G binary plaintext can be decrypted continuously and stably, with an average BER of 9.57e-4, which can be further corrected by forward error correction (FEC).

In this study, the BER of the illegitimate receiver is measured through offline comparison in the Integrated Logic Analyzer (ILA). Due to the limitation of BERT, which cannot measure BER beyond 1e-3, the BER value of the illegitimate receiver cannot be directly obtained. Calculated offline, BER of the illegitimate receiver is approximately 0.5, which shows that the security is guaranteed. It is worth noting that the transmission distance is limited by OMs, which are designed for short-distance applications.

Conclusions

In this paper, we demonstrated an all-digital FPGA-based real-time QNSC transmission for a typical bidirectional CWDM system supporting 8 users. By applying DSM, transmitting the 2-level optical signal over the fiber link allows the entire encryption and decryption process to be implemented without any analog components. Moreover, the receiver utilizes a simple CDR algorithm without an extra link for clock signal. Continuous data processing and BERT monitoring prove that the proposed optical module-based QNSC scheme is compatible with existing short reach and multi-user access networks such as wireless fronthaul and optical access network. This physical layer secure system can truly achieve protocol-transparent and plug-and-play functionality. Meanwhile, the dynamic changes of key seed patterns and DSM parameters enhance the practicability and security of this scheme.

Acknowledgements

This work was supported by the National Key Research and Development Program of China (2021YFB1808200); National Natural Science Foundation of China (62275091, 62205115).

References

[1] A. Zhao, N. Jiang, S. Liu, Y. Zhang and K. Qiu, "Physical Layer Encryption for WDM Optical Communication Systems Using Private Chaotic Phase Scrambling," *Journal of Lightwave Technology*, vol. 39, no. 8, pp. 2288-2295, 2021, DOI: 10.1109/JLT.2021.3051407.

[2] X. Chen, K. Tanizawa, P. Winzer, P. Dong, J. Cho, F. Futami, K. Kato, A. Melikyan, and K. W. Kim, "Experimental demonstration of a 4,294,967,296-QAM-based Y-00 quantum stream cipher template carrying 160-Gb/s 16-QAM signals," *Optics Express*, vol. 29, no. 4, pp. 5658-5664, 2021, DOI: 10.1364/OE.405390.

[3] K. Tanizawa and F. Futami, "Ultra-long-haul digital coherent PSK Y-00 quantum stream cipher transmission system," *Optics Express*, vol. 29, no. 7, pp. 10451-10464, 2021, DOI: 10.1364/OE.418302.

[4] J. Sun, L. Jiang, A. Yi, J. Feng, X. Deng, W. Pan, B. Luo, and L. Yan, "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," *Optics Express*, vol. 31, no. 7, pp. 11344-11353, 2023, DOI: 10.1364/OE.484431.

[5] M. Yoshida, T. Hirooka, K. Kasai, and M. Nakazawa, "Real-time 10 Gbit/s-16 QAM Quantum Stream Cipher Transmission over 320 km with FPGA-based Transmitter and Receiver," in *Optical Fiber Communication Conference (OFC)*, Los Angeles, United States, 2015, paper W4F.4, DOI: 10.1364/OFC.2015.W4F.4.

[6] M. Yoshida, T. Hirooka, K. Kasai and M. Nakazawa, "Real-time adaptive 4–64 QAM, 20–60 Gbit/s quantum noise stream cipher transmission over 320 km with FPGA-based transmitter and receiver," in *European Conference on Optical Communication (ECOC)*, Valencia, Spain, 2015, pp. 1-3, DOI: 10.1109/ECOC.2015.7341787.

[7] M. Yoshida, T. Kan, K. Kasai, T. Hirooka and M. Nakazawa, "10 Tbit/s QAM Quantum Noise Stream Cipher Coherent Transmission Over 160 Km," *Journal of Lightwave Technology*, vol. 39, no. 4, pp. 1056-1063, 2021, DOI: 10.1109/JLT.2020.3016693.

[8] H. Luo, L. Zhong, S. Zhang, X. Dai, L. Deng, D. Liu, M. Cheng and Q. Yang, "DAC/ADC-free 65536-level Quantum Noise Stream Cipher for Secure Fiber Transmission based on Delta-Sigma Modulation," in *European Conference on Optical Communication (ECOC)*, Basel, Switzerland, 2022, paper. Tu1C.5.

[9] L. Liu, J. Xie, F. Pan, B. Wu and W. Zhao. "Investigation and evaluation of 25 Gb/s optical modules for 5G fronthaul." *Optical Design and Testing X*, vol. 11548, pp. 203-208. SPIE, 2020, DOI: 10.1117/12.2573910

[10] D. Zhang, Z. Du, M. Cheng, M. Jiang and X. Liu, "Innovation and Demonstration of a New CWDM and Circulator Integrated Semi-Active System for 5G Fronthaul," *Journal of Lightwave Technology*, vol. 41, no. 4, pp. 1223-1229, 2023, DOI: 10.1109/JLT.2022.3199470.

[11] J. Wang, Z. Jia, L. A. Campos and C. Knittle, "Delta-Sigma Modulation for Next Generation Fronthaul Interface," *Journal of Lightwave Technology*, vol. 37, no. 12, pp. 2838-2850, 2019, doi: 10.1109/JLT.2018.2872057.

[12] Spectral Grids for WDM Applications: CWDM Wavelength Grid, ITU-T G.694.2, International Telecommunication Union, Geneva, Switzerland, 2003

[13] X. Liu and N. Deng, “Emerging optical communication technologies for 5G,” in Chapter 17 of Optical Fiber Telecommunications VII, ed. by A. Willner, Ed., New York, NY, USA: Academic Press, 2019. DOI: 10.1016/B978-0-12-816502-7.00019-1.

[14] X. Chen et al., "Feasibility of 25Gb/s MWDM Transmission Over a 15-km G652.D Compliant Fiber for 5G Fronthaul Networks," in *Opto-Electronics and Communications Conference (OECC)*, Hong Kong, China, 2021, paper T2C.7.

[15] L. Zhong, Y. Zou, S. Zhang, X. Dai, J. Zhang, M. Cheng, L. Deng, Q. Yang, and D. Liu, "An SNR-improved Transmitter of Delta-sigma Modulation Supported Ultra-High-Order QAM Signal for Fronthaul/WiFi Applications," *Journal of Lightwave Technology*, vol. 40, no. 9, pp. 2780-2790, 2022, DOI: 10.1109/JLT.2022.3147059.