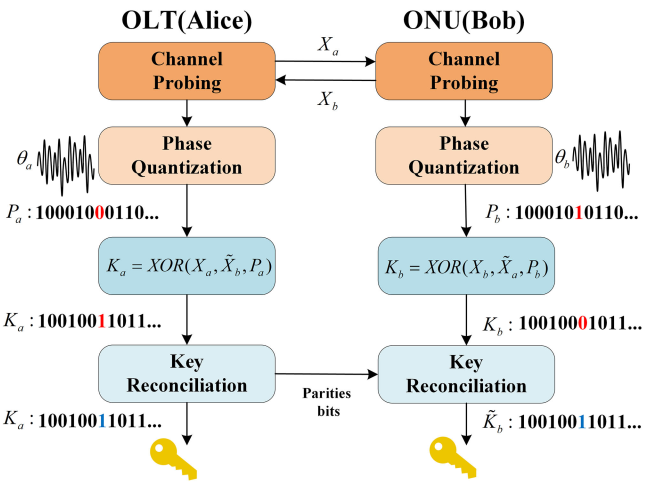
IEEE Photonics Journal
An IEEE Photonics Society Publication

Open Access

# Channel-Based Dynamic Key Generation for Physical Layer Security in OFDM-PON Systems

Volume 13, Number 2, April 2021

Yating Wu
Yan Yu
Yuanfeng Hu
Yanzan Sun
Tao Wang
Qianwu Zhang



DOI: 10.1109/JPHOT.2021.3056053

# Channel-Based Dynamic Key Generation for Physical Layer Security in OFDM-PON Systems

**Yating Wu, Yan Yu, Yuanfeng Hu, Yanzan Sun, Tao Wang, and Qianwu Zhang**

Key Laboratory of Specialty Fiber Optics and Optical Access Networks, Joint International Research Laboratory of Specialty Fiber Optics and Advanced Communication, Shanghai University, Shanghai 200444, China

*DOI:10.1109/JPHOT.2021.3056053*

*This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/*

Manuscript received October 26, 2020; revised December 30, 2020; accepted January 27, 2021. Date of publication February 4, 2021; date of current version March 10, 2021. This work was supported in part by the Science and Technology Commission of Shanghai Municipality (Project 20511102400, 20ZR1420900), in part by 111 project (D20031), and in part by the National Natural Science Foundation of China (NSFC No. 61671011). Corresponding author: Tao Wang (e-mail: twang@shu.edu.cn).

**Abstract:** Key generation and distribution is a fundamental problem of communication security. To avoid the potential risk due to static key, a physical-layer dynamic key generation and encryption scheme is proposed for orthogonal frequency division multiplexing passive optical network (OFDM-PON) systems. By exploiting the inherent channel randomness, the shared secret key between the OLT and ONU is generated and renewed periodically, thereby effectively improving the security against malicious attacks. The transmission experiment of 3.5 Gb/s 16-quardrature-amplitued-modulatin encrypted OFDM data is successfully demonstrated over a 25 km standard single-mode fiber. The key space of the proposed encryption scheme reaches $10^{66}$, which provides privacy between users and protection against eavesdropping.

**Index Terms:** Orthogonal frequency division multiplexing (OFDM), passive optical network (PON), key generation, security.

## 1. Introduction

With the ever-growing data traffic of all kinds of applications and cloud services, security in optical networks has become a crucial issue of worldwide concern. Orthogonal frequency division multiplexing passive optical network (OFDM-PON) has emerged as an attractive candidate for next-generation broadband optical access due to its numerous advantages such as high spectral efficiency, fine bandwidth granularity, strong robustness to chromatic dispersion, and great flexibility in dynamic bandwidth allocation [1], [2]. Several OFDM-PON systems capable of ultra-high data rates have been reported and demonstrated [3]–[5]. However, due to the reflection effect at the power splitters and the broadcast nature of PON, the data is vulnerable to eavesdropping attacks by malicious users [6], [7].

Apart from the security measures based on cryptographic algorithms and authentication protocols at MAC or higher layers, security employed on physical layer provides a secure foundation for a robust network [8], which is transparent for different types of data. Physical-layer security

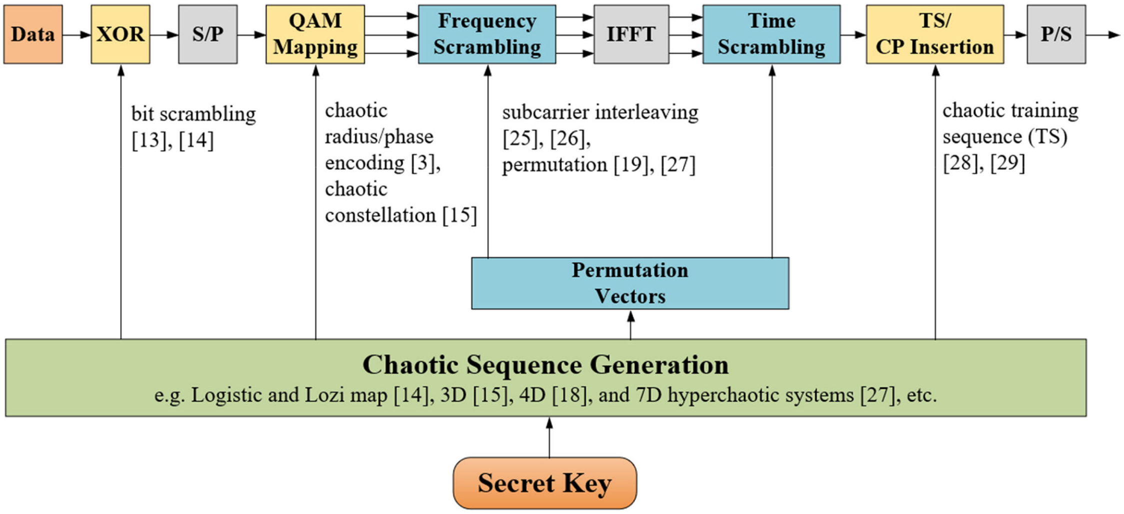

Data
XOR
S/P
QAM Mapping
Frequency Scrambling
IFFT
Time Scrambling
TS/ CP Insertion
P/S
bit scrambling [13], [14]
chaotic radius/phase encoding [3], chaotic constellation [15]
subcarrier interleaving [25], [26], permutation [19], [27]
chaotic training sequence (TS) [28], [29]
Permutation Vectors
Chaotic Sequence Generation
e.g. Logistic and Lozi map [14], 3D [15], 4D [18], and 7D hyperchaotic systems [27], etc.
Secret Key

Fig. 1. Block diagram of existing chaos-based encryption schemes for OFDM-PON systems.

in PONs can be implemented in optical domain [9]–[12] or electric domain [13]–[15]. For most optical encryption schemes, the key space is often limited due to the restricted range of physical parameters [10]. Moreover, the use of costly optical components such as quantum light sources and femtosecond lasers are generally required [16].

In recent years, considerable efforts have been devoted to physical-layer security enhancement using digital signal processing (DSP) approaches in electric domain for OFDM-PON system [17]–[29]. In particular, chaotic encryption has been widely investigated owing to its desirable properties such as ergodicity, sensitivity to the initial values and low implementation cost [17]–[24]. For example, the OFDM symbols are divided into sub-matrices and encrypted by different algorithms based on chaotic systems [21]–[23]. The block diagram shown in Fig. 1 provides a summary of the existing chaos-based encryption schemes for OFDM-PON systems, where chaos has been applied at different stages in the system. The chaotic sequences can be used for bit scrambling, constellation shifting, or to control the frequencies of RF subcarriers [24], etc.

It is worth noting that regardless of the specific encryption methods, the key plays a critical role as it is the seed of the chaotic sequences used in the subsequent encryption. However, few of the aforementioned research works considered the key generation problem and most works assumed a static secret key between the OLT and the ONU, which makes the system vulnerable to statistical analysis attack [4] and known-plaintext attacks (KPAs) [30].

Therefore, in this paper, we propose a channel-based dynamic key generation scheme for physical layer security in OFDM-PON systems. The principal idea is to exploit the inherent channel randomness associated with each distinct pairwise communication link. The shared secret key between the OLT and ONU is generated and renewed periodically by combining the randomness of the channel phase response and locally-generated random signal. A keys pace of $\sim 10^{66}$ is achieved which enhances the security effectively. Reconciliation using error correcting codes is employed to correct key discrepancy due to the noise and channel measurement errors, ensuring that the generated shared keys on both sides are consistent with each other. Simulations and a real-time IM/DD OFDM-PON system are set up to verify the performance experimentally.

The rest of this paper is organized as follows. Section 2 presents the principle of the proposed key generation and encryption scheme. Simulation and experimental results based on a real-time IM/DD OFDM-PON system are provided in Section 3. Finally, conclusions are drawn in Section 4.

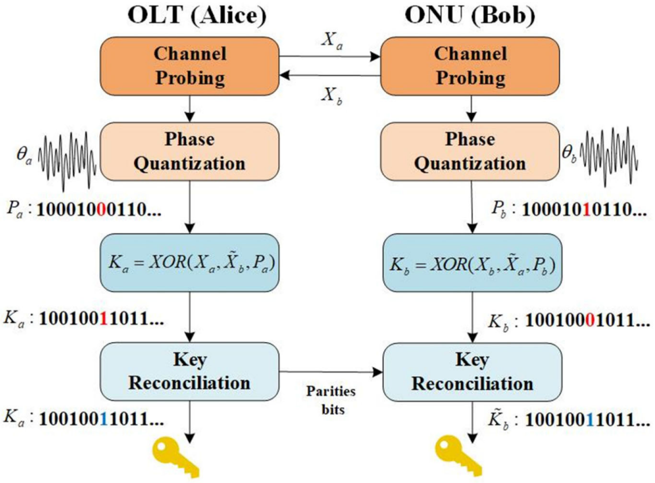


Fig. 2. Key generation procedures.

## 2. Principle

The process of the proposed dynamic key generation scheme is illustrated in Fig. 2. Three key steps are involved, including channel probing, phase quantization, and key reconciliation.

Consider two parties OLT (Alice) and ONU (Bob) that want to generate a shared secret key between them in the presence of an eavesdropper. The cryptographic key needs to be as random as possible to make it infeasible for the eavesdropper to predict or reproduce the key. In this paper, the randomness comes from two sources, which are the channel variation and the locally generated random signal.

### *2.1 Channel Probing*

During channel probing, Alice and Bob exchange random probing signals with each other. The random signals serve a two-fold purpose, which is to facilitate the channel measurement and enhance the randomness of the key as well. Both parties estimate and record the phases of the common channel in the pairwise communication link. The system equation is given by

$$\boldsymbol{y}_B = \boldsymbol{H}_{AB}\,\boldsymbol{x}_A + \boldsymbol{n}_B \tag{1}$$

$$\boldsymbol{y}_A = \boldsymbol{H}_{BA}\,\boldsymbol{x_B} + \boldsymbol{n}_A \tag{2}$$

where $\boldsymbol{x}$ and $\mathbf{y}$ denote the transmitted and received signal vectors, $\boldsymbol{H} = [H_1, H_2 \cdots, H_n] \in \mathrm{C}^{\mathrm{N}\times\mathrm{N}}$, denotes the channel matrix and $n$ denotes the $N$-dimensional vector of noise and interference. The channel probing is done within one channel coherence time interval, over which the channel impulse response is essentially invariant. In this paper, we assume reciprocal channels, i.e., $\boldsymbol{H}_{AB} = \boldsymbol{H}_{BA}$ during the coherence time, where Alice and Bob observe highly correlated channels.

### *2.2 Phase Quantization*

After channel estimation, both Alice and Bob extract key bits from estimated channel phases using a quantizer. The channel phases of selected $S$ subcarriers $\theta = \{\theta_1\theta_2\cdots\theta_s\}$, $(\theta_i \in [0,\ 2\pi),\ i = 1,\ 2, \ldots, S)$ are selected and uniformly quantized into $Q$ levels. The quantized bits on each side are then concatenated to yield a random phase sequence $P_a$ and $P_b$ of $Slog_2Q$ bits, respectively.

The final key is generated by applying the $XOR$ operation among the locally generated random sequence, the received random sequence and the quantized phase sequence, which can be written

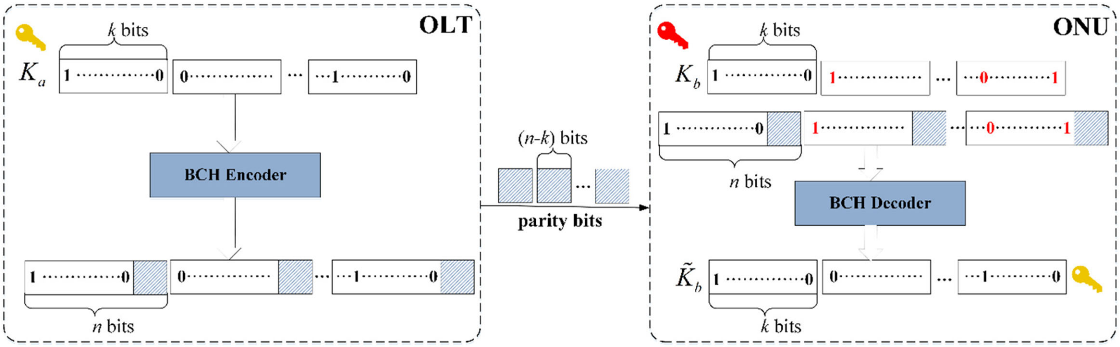


Fig. 3. Key reconciliation based on BCH codes.

as

$$K_a = X_a \oplus \tilde{X}_b \oplus P_a \tag{3}$$

$$K_b = X_b \oplus \tilde{X}_a \oplus P_b \tag{4}$$

where $\oplus$ denotes the $XOR$ operation, $K_a$ denotes the key of Alice, and $K_b$ denotes the key of Bob. $\tilde{X}_b$ and $\tilde{X}_a$ denote the random sequences received by Alice and Bob, respectively.

The key generation rate of the proposed scheme mainly depends on the number of selected subcarriers and phase quantization levels, the channel probing rate, and the channel conditions which determines the amount of randomness available for extraction. Note that there is a tradeoff in determining the number of quantization levels $Q$. While higher value of $Q$ leads to finer quantized phase information and hence higher key generation rate, it also increases the probability of bit disagreement between the two sides.

### 2.3 Key Reconciliation

Due to the hardware variations, noise and channel estimation errors, there may exist some bit discrepancies between the generated keys of two parties. In order to achieve key agreement, reconciliation must be employed to correct the bit discrepancies. In this paper, we propose a reconciliation method based on Bose-Chaudhuri-Hocquenghem (BCH) code. BCH code [31] is a class of linear cyclic block codes, which is known for its error correcting ability and ease of encoding and decoding.

A $(n,\ k,\ t)$ BCH code is used in the key reconciliation scheme, where $n$, $k$ and $t$ represent the codeword length, the information bit length and the error correction capability, respectively. During reconciliation, parity bit information is sent to correct errors. Such parity information enables the ONU to identify and correct the mismatching bits, as illustrated in Fig. 3.

The procedures of the reconciliation are as follows:

1) OLT divides its key $K_a$ with length of $Slog_2Q$ bits into $\lceil Slog_2Q/k \rceil$ $k$-bit blocks and feeds them into the $(n,\ k,\ t)$ BCH encoder. Each output codeword contains two parts, which are the $k$-bit message bits and the $(n-k)$-bit parity bits.
2) OLT sends the parity bits to ONU.
3) ONU combines its own key $K_b$ with the received parity bits to form $\lceil Slog_2Q/k \rceil$ codewords with code length of $n$ bits, which are then fed into the BCH decoder. Finally, the reconciled key $\tilde{K}_b$ is obtained by the output of the decoder.

The proposed reconciliation can correct up to $\lceil Slog_2Q/k \rceil t$ bit discrepancies between $K_a$ and $K_b$. If the mismatch between $K_a$ and $K_b$ is within $\lceil Slog_2Q/k \rceil t$ bits, the keys on both sides would be identical with each other. i.e., $\tilde{K}_b = K_a$. As listed in Table 1, BCH code offers different combinations of code rate and error correction ability. A bigger value of $t$ can correct more errors but with the cost of an

TABLE 1
BCH Code Parameters $(n,\ k,\ t)$

| Codeword length $n$ | Information bit length $k$ | Error correction capability $t$ |
|---|---|---|
| 7 | 4 | 1 |
| 15 | 11 | 1 |
| | 7 | 2 |
| | 5 | 3 |
| 31 | 26 | 1 |
| | 21 | 2 |
| | 16 | 3 |
| | 11 | 5 |
| | 6 | 7 |
| 63 | 57 | 1 |
| | 51 | 2 |
| | 45 | 3 |
| | 39 | 4 |
| | 36 | 5 |

increased overhead. For example, for a 78-bit key, it can either use three BCH (31, 26, 1) or two BCH (63, 39, 4) encoders and decoders. The former can provide a 3-bit error correction capability, while the latter can correct up to 8-bit errors.

### *2.4 Data Encryption*

After reconciliation, OLT and ONU would share the same secret key, which is used to encrypt the subsequent data. The aforementioned existing chaos-based encryption techniques listed in Fig. 1 can be applied to convert the key into cryptographic sequences such as chaotic scrambling bits or permutation vectors. For simplicity, a one-dimensional logistic chaotic map is employed to generate the keystream sequence, which can be expressed by

$$x_{n+1} = \mu x_n (1 - x_n),\ x_n \in (0,\ 1),\ \mu \in [1,\ 4] \tag{5}$$

where $n$ represents the $n$-th iteration, and $\mu$ denotes the bifurcation parameter. It has been demonstrated that when $\mu \in\ (3.574,\ 4]$ , the whole system enters a state of chaos.

The key serves as the initial values of the chaotic system, which outputs the chaotic sequence as the keystream $K_s$ to encrypt or decrypt the data. As shown in Fig. 4, even a tiny change of the initial value ($\sim 10^{-15}$) would result in a totally different chaotic state, which indicates that the generated cryptographic key stream is highly sensitive to the key. The data encryption is implemented by applied the $XOR$ operation between the key stream and the data, i.e.,

$$\tilde{D} = K_S\ \oplus D \tag{6}$$

where $D$ is the original downlink data stream and $\tilde{D}$ is the downstream data stream encrypted by the key stream.

The decryption is done by the inverse operations. Therefore, only the legitimate ONU with exactly the same key can generate the right keystream and recover the data.

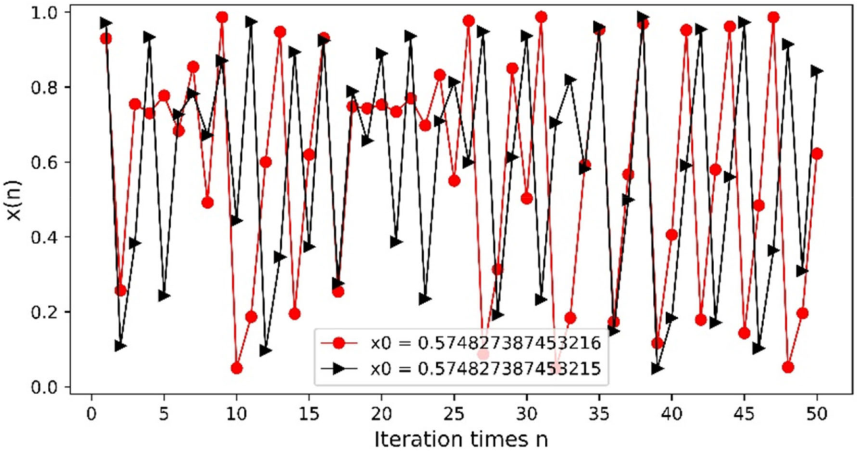
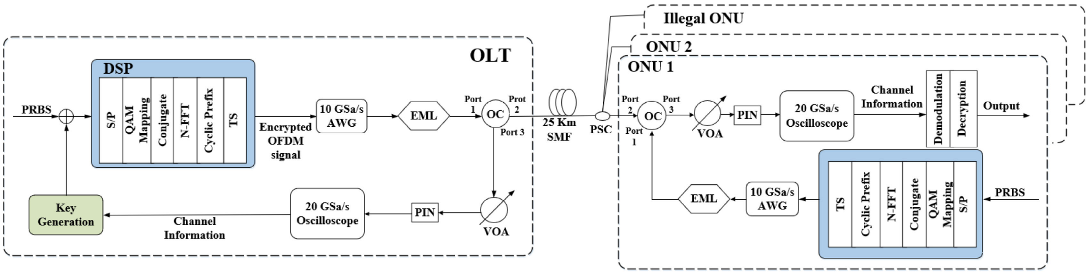


Fig. 4. Sensitivity of the chaotic sequences to the initial condition.



AWG: Arbitrary waveform generator; EML: Electro absorption modulated distributed feedback laser; OC: Optical Circulator; VOA: Variable Optical Attenuator; PIN: Positive Intrinsic-Negative; S/P: Serial-to-parallel; PSC: Power Splitter/Coupler; DSP: Digital Signal Processing.

Fig. 5. Experimental setup for the proposed OFDM-PON encryption system.

## 3. Experimental Setup and Results

To experimentally verify the security performance of the proposed scheme, we set up a real-time intensity modulation direct detection (IMDD) OFDM-PON system as shown in Fig. 5. The key system parameters are summarized in Table 2. Real-time transmitter and receiver are realized using Virtex-6 FPGA from Xilinx with fully pipelined DSP architecture.

At the stage of key generation, OLT and legal ONU (ONU1) send random signal to each other for channel probing. An Electro-absorption Modulated Laser (EML) of the central wavelength at 1500 nm is used as the optical source. The generated optical OFDM signals transmitted through an Optical Circulator (OC) and over 25 km standard single-mode fiber (SSMF). At the receiving side, the signals are received via a Positive Intrinsic-Negative (PIN) of 1.5 GHz bandwidth and recorded by a 20 Gs/s real-time oscilloscope for offline processing. The line rate in the experiment is 3.5 Gb/s ($56/64\times\log_2 16$).

A Pseudo Random Binary Sequence (PRBS)-15 is generated by MATLAB as the original data. Key $K_a$ serves as the seed of the chaotic system, and generates the chaotic sequence $K_s$ as the keystream. The data encryption is implemented by applied the XOR operation between the keystream and the data. After serial-to-parallel (S/P), these data are modulated into 16QAM OFDM signals. The encrypted data is uploaded into the AWG with 2 GSa/s sampling rate to generate electrical OFDM signals, and drive the EML at 1550 nm. The modulated optical signals are transmitted through an OC and 25 km SSMF. At ONU, the signals are received via a PIN of 1.5 GHz bandwidth and recorded by a real-time oscilloscope for offline processing.

TABLE 2
System Parameters Used for OFDM-PON Encryption System

| Parameter | Value |
|---|---|
| Modulation format | 16QAM |
| FFT/IFFT points | 64 |
| Cyclic prefix | 16 Samples |
| Number of OFDM symbols per frame | 100 |
| Data-carrying subcarriers | 56 |
| Data rate | 3.5Gb/s |
| AWG sampling rate | 2 GSa/s |
| EML wavelength | 1550 nm |
| Fiber length | 25 km |
| PIN detector bandwidth | 12 GHz |

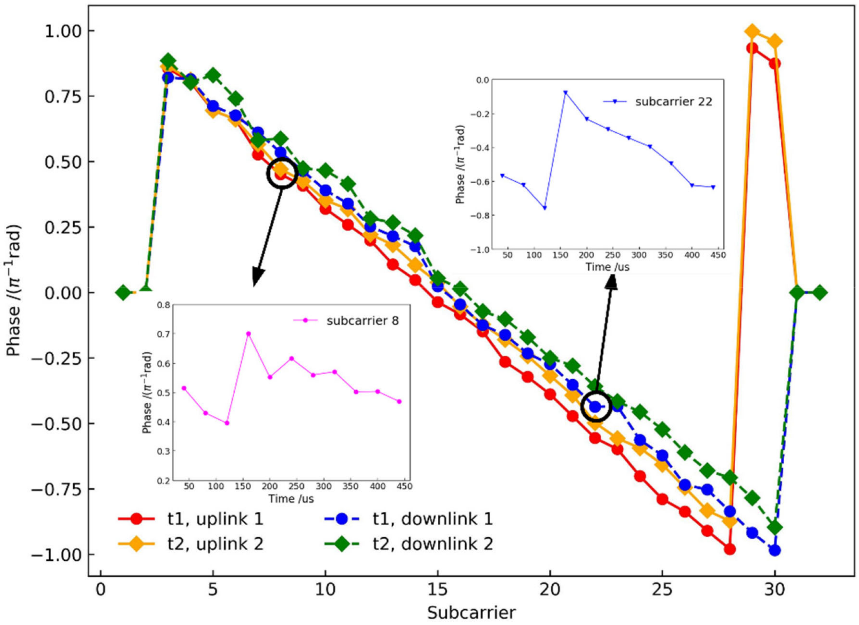
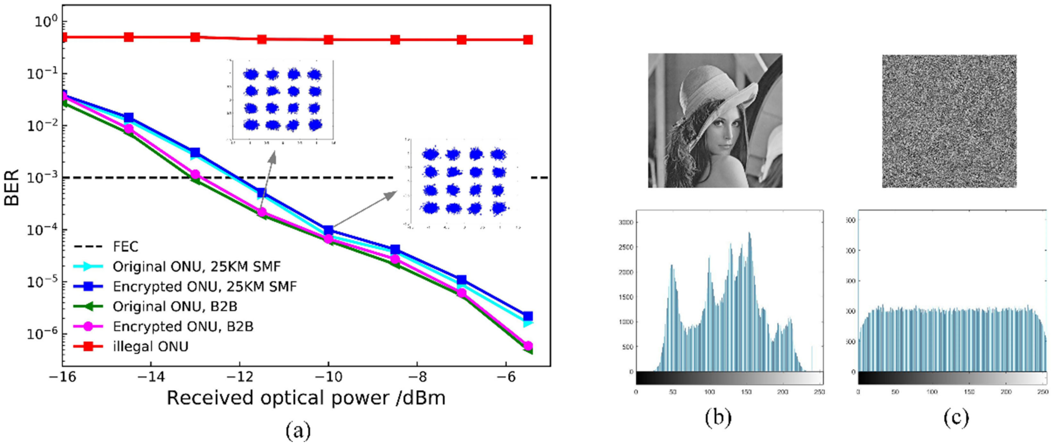


Fig. 6. Uplink and downlink channel phase.

During the channel quantization, the channel phases of 19 subcarriers are selected and uniformly quantized into $2^3$ levels. The quantized bits are then concatenated to yield phase sequences $P_a$ and $P_b$ of 57 bits for each side, respectively. The secure key $K_a$ and $\mathrm{K_b}$ is then obtained by applying the $XOR$ operation among the quantized phase sequence, received and locally generated random sequences. During reconciliation, $K_a$ is fed into BCH (63, 57, 1) encoder and the parity bits are sent to ONU through the public channel. The received parity bits are attached to key $K_b$ to form a new codeword, which is sent into BCH decoder. Finally, ONU obtains the reconciled 57-bit key $\tilde{K}_b$ by the output of the decoder, which created a key space of $2^{57} \times 2^{57} \times 2^{57}$ ($\sim 10^{51}$). The cryptographic chaotic sequence offers an additional key space of $10^{15}$. Hence, the total key space of the proposed encryption scheme $\sim 10^{66}$ (i.e., $2^{57} \times 2^{57} \times 2^{57} \times 10^{15}$), which provides high security against brute force attacks. Note that the key space can be readily enhanced simply by increasing the number of selected subcarriers and quantization levels.



(a)

(b)

(c)

Fig. 7. (a) Measured BER of encrypted and original OFDM-PON systems; Image and Histogram of (b) intended ONU and (c) illegal ONU.

The experimental results in Fig. 6 show that the channel phase changes with time, which can be a source of dynamic randomness. The uplink phases are close to downlink phases, hence channel reciprocity holds after reconciliation.

Fig. 7 exhibits the bit error rate (BER) performance of the proposed encryption scheme for OFDM-PON systems after back-to-back (B2B) transmission and 25 km SSMF transmission, respectively. A classical digital image is used as an example to illustrate the encryption effect. For the legitimate ONU with the correct key, the OFDM signal can be correctly decrypted after transmission, while the illegal ONU ends up with a BER of ∼0.5, indicating that illegal user is incapable of recovering any effective information from the downlink signal. As shown, the image is scrambled and hidden from the illegal ONU, while the intended ONU can recover the image correctly using the shared secret key with OLT. The error rate of the encrypted system is slightly higher than that of the original unencrypted system due to the possible errors in the estimation and quantization of the phase information at both ends which may cause key discrepancies. In summary, the proposed encryption scheme can enhance the security of the system while not affecting the transmission performance.

## 4. Conclusion

We have proposed and experimentally demonstrated a channel-based dynamic key generation to enhance the physical layer security for OFDM-PON systems. By combining the randomness of the channel phase response and locally-generated random signal, a shared secret key between the OLT and ONU is generated and updated periodically. Reconciliation using BCH error correcting codes is employed to keep the generated shared keys on both sides consistent with each other. Experimental results show that the proposed scheme can effectively prevent eavesdropping and enhance the security of OFDM-PON system.

## References

[1] N. Cvijetic, “OFDM for next-generation optical access networks,” *J. Lightw. Technol.*, vol. 30, no. 4, pp. 384–389, Feb. 2012.

[2] H. S. Abbas and M. A. Gregory, “The next generation of passive optical networks: A review,” *J. Netw. Comput. Appl.*, vol. 67, pp. 53–74, May. 2016.

[3] A. Sultan, X. Yang, A. A. E. Hajomer, and W. Hu, “Chaotic constellation mapping for physical-layer data encryption in OFDM-PON,” *IEEE Photon. Technol. Lett.*, vol. 30, no. 4, pp. 339–341, Feb. 2018.

[4] W. Zhang, C. Zhang, C. Chen, and K. Qiu, “Experimental demonstration of security-enhanced OFDMA-PON using chaotic constellation transformation and pilot-aided secure key agreement,” *J. Lightw. Technol.*, vol. 35, no. 9, pp. 1524–1530, May 2017.

[5] Q. Chen, M. Bi, X. Fu, Y. Lu, and S. Xiao, “Security scheme in IMDD-OFDM-PON system with the chaotic pilot interval and scrambling,” *Opt. Commun.*, vol. 407, no. 16, pp. 285–289, Jan. 2018.

[6] D. Gutierrez, J. Cho, and L. G. Kazovsky, “TDM-PON security issues: Upstream encryption is needed,” in *Proc. Nat. Fiber Optic Engineers Conf.*, Anaheim, CA, USA, Mar. 2007, pp. 1–3.

[7] K. Shaneman and S. Gray, “Optical network security: Technical analysis of fiber tapping mechanisms and methods for detection & prevention,” in *Proc. IEEE Mil. Commun. Conf.*, 2004, pp. 711–716.

[8] N. Skorin-Kapov, M. Furdek, S. Zsigmond, and L. Wosinska, “Physical-layer security in evolving optical networks,” *IEEE Commun. Mag.*, vol. 54, no. 8, pp. 110–117, Aug. 2018.

[9] M. P. Fok, Z. Wang, Y. Deng, and P. R. Prucnal, “Optical layer security in fiber-optic networks,” *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 725–736, Sep. 2011.

[10] Y. Huang, H. Chen, H. Huang, N. K. Fontaine, and M. Wang, “Temporal and spectral coding over amplified spontaneous emission (ASE) for secure optical coherent communications,” *Opt. Lett.*, vol. 45, no. 4, pp. 1039–1042, Jan. 2020.

[11] A. Zhao, N. Jiang, S. Liu, Y. Zhang, and K. Qiu, “Generation of synchronized wideband complex signals and its application in secure optical communication,” *Opt. Exp.*, vol. 28, no. 16, pp. 23363–23373, Jul. 2020.

[12] Y. Fu *et al.*, “High-speed optical secure communication with an external noise source and an internal time-delayed feedback loop,” *Photon. Res.*, vol. 7, no. 11, pp. 1306–1313, Oct. 2019.

[13] P. Cao, X. Hu, J. Wu, L. Zhang, X. Jiang, and Y. Su, “Physical layer encryption in OFDM-PON employing time-variable keys from ONUs,” *IEEE Photon. J.*, vol. 6, no. 2, Apr. 2014, Art. no. 7901006.

[14] L. Zhang, X. Xin, B. Liu, and Y. Wang, “Secure OFDM-PON based on chaos scrambling,” *IEEE Photon. Technol. Lett.*, vol. 23, no. 14, pp. 998–1000, May. 2011.

[15] L. Zhang, B. Liu, X. Xin, and D. Liu, “A novel 3D constellation-masked method for physical security in hierarchical OFDMA system,” *Opt. Exp.*, vol. 21, no. 13, pp. 15627–15633, Jun. 2013.

[16] T. S. Humble, “Quantum security for the physical layer,” *IEEE Commun. Mag.*, vol. 51, no. 8, pp. 56–62, Aug. 2013.

[17] A. Sultan, X. Yang, A. A. E. Hajomer, S. B. Hussain, and W. Hu, “Dynamic QAM mapping for physical-layer security using digital chaos,” *IEEE Access*, vol. 6, pp. 47199–47205, Aug. 2018.

[18] M. Cheng *et al.*, “Enhanced secure strategy for OFDM-PON system by using hyperchaotic system and fractional Fourier transformation,” *IEEE Photon. J.*, vol. 6, no. 6, Oct. 2014, Art. no. 7903409.

[19] M. Bi *et al.*, “A key space enhanced chaotic encryption scheme for physical layer security in OFDM-PON,” *IEEE Photon. J.*, vol. 9, no. 1, Feb. 2017, Art. no. 7901510.

[20] C. Zhang, W. Zhang, C. Chen, X. He, and K. Qiu, “Physical-enhanced secure strategy for OFDMA-PON using chaos and deoxyribonucleic acid encoding,” *J. Lightw. Technol.*, vol. 36, no. 9, pp. 1–10, Jan. 2018.

[21] T. Wu, C. Zhang, H. Wei, and K. Qiu, “PAPR and security in OFDM-PON via optimum block dividing with dynamic key and 2D-LASM,” *Opt. Exp.*, vol. 27, no. 20, pp. 27946–27960, Sep. 2019.

[22] H. Wei, C. Zhang, T. Wu, H. Huang, and K. Qiu, “Chaotic multilevel separated encryption for security enhancement of OFDM-PON,” *IEEE Access*, vol. 7, no. 6, pp. 124452–124460, Sep. 2019.

[23] T. *et al.*, “Security enhancement for OFDM-PON using brownian motion and chaos in cell,” *Opt. Exp.*, vol. 26, no. 18, pp. 22857–22865, Aug. 2018.

[24] C. Zhang, W. Zhang, X. He, C. Chen, H. Zhang, and K. Qiu, “Physically secured optical OFDM-PON by employing chaotic pseudorandom RF subcarriers,” *IEEE Photon. J.*, vol. 9, no. 5, Oct. 2017, Art. no. 7204408.

[25] W. Zhang, C. Zhang, W. Jin, K. Qiu, and C. Chen, “Hybrid time-frequency domain chaotic interleaving for physical-layer security enhancement in OFDM-PON systems,” in *Proc. IEEE/CIC Int. Conf. Commun. China.*, Chengdu, China, 2016, pp. 1–4.

[26] L. Zhang, B. Liu, X. Xin, Q. Zhang, J. Yu, and Y. Wang, “Theory and performance analyses in secure CO-OFDM transmission system based on two-dimensional permutation,” *J. Lightw. Technol.*, vol. 31, no. 1, pp. 74–80, Oct. 2013.

[27] Z. Hu and C. K. Chan, “A 7-D hyperchaotic system-based encryption scheme for secure Fast-OFDM-PON,” *J. Lightw. Technol.*, vol. 36, no. 16, pp. 3373–3381, May. 2018.

[28] L. Deng *et al.*, “Secure OFDM-PON system based on chaos and fractional Fourier transform techniques,” *J. Lightw. Technol.*, vol. 32, no. 15, pp. 2629–2635, Jun. 2014.

[29] S. Li *et al.*, “Secure key distribution strategy in OFDM-PON by utilizing the redundancy of training symbol and digital chaos technique,” *IEEE Photon. J.*, vol. 10, no. 2, Apr. 2014, Art. no. 7201108.

[30] Y. M. Al-Moliki, M. T. Alresheedi, and Y. Al-Harthi, “Physical-layer security against known/chosen plaintext attacks for OFDM-Based VLC system,” *IEEE Commun. Lett.*, vol. 21, no. 12, pp. 2606–2609, Dec. 2017.

[31] R. T. Chien, “Cyclic decoding procedures for Bose-Chaudhuri-Hocquenghem codes,” *IEEE Trans. Inf. Theory*, vol. 10, no. 4, pp. 357–363, Oct. 1964.