IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received July 15, 2018, accepted August 17, 2018, date of publication August 23, 2018, date of current version September 21, 2018.

Digital Object Identifier 10.1109/ACCESS.2018.2866797

Dynamic QAM Mapping for Physical-Layer Security Using Digital Chaos

AMBER SULTAN, XUELIN YANG, ADNAN A. E. HAJOMER, SYED B. HUSSAIN, AND WEISHENG HU
Shanghai Institute for Advanced Communication and Data Science, State Key Laboratory of Advanced Optical Communication Systems and Networks,
Shanghai Jiao Tong University, Shanghai 200240, China

Corresponding author: Xuelin Yang (x.yang@sjtu.edu.cn)

This work was supported in part by the Ministry of Science and Technology of China under Grant 2016YFE0104500 and in part by the Natural Science Foundation of China Grants 61571291, 61431009, 61433009, and 61221001.

ABSTRACT This paper proposes and experimentally demonstrates a physical-layer data encryption scheme using multi-fold chaotic mapping of quadrature amplitude modulation (QAM) symbols in orthogonal frequency-division-multiplexed passive optical network (OFDM-PON). Dynamic radius and phase offsets are added in the standard QAM during QAM mapping on constellation using digital chaos. Due to the dynamic chaotic radius and phase offsets, the QAM symbols are mapped over the entire constellation plane, and thus the random, flexible QAM mapping is reconstructed to provide high-level security during data transmission. Since the chaotic offsets along with the data permutations are independently predetermined by a hyper digital chaos, the multi-fold data encryption creates an overall key space of $\sim 10^{340}$ to enhance the physical-layer security. Successful transmission experiment of 9.4-Gb/s, 16-QAM encrypted OFDM data is demonstrated over a 22-km standard single-mode fiber in OFDM-PON. Moreover, with the use of dynamic mapping of QAM symbols, the transmission performance is not significantly degraded after implementing the proposed multi-fold secure data encryption.

INDEX TERMS Digital chaos, orthogonal frequency-division multiplexing (OFDM), passive optical network (PON).

I. INTRODUCTION

The fast-paced advancement in internet technologies has led to serious consideration about the spectrum availability in passive optical networks (PONs) [1]. In order to deal with this capacity crunch, orthogonal frequency division multiplexing (OFDM) with its properties of spectral efficiency, resistance to fiber dispersion and dynamic resource allocation, is a desirable candidate for future PONs [2]. However, the architecture of PONs brings forth a serious issue of user data security. Since PONs have a broadcasting nature during downstream transmission, user data can be easily eavesdropped. Currently, data encryption in media access control (MAC) layer is unable to protect the header of the transmitted data, and provides the possibility of decrypting the entire data by an illegal optical network unit (ONU). Therefore, physical-layer encryption is required to enhance the security of downstream data transmission in PONs [3].

Digital chaos, owing to its properties such as sensitivity to initial value and ergodicity, is ideal to serve as data encryption technique [4], [5]. Several physical-layer encryption schemes have incorporated digital chaos to enhance the security of downstream transmission in OFDM-PON, where standard QAM has been employed. In [6], secure data encryption is provided by using chaotic Walsh-Hadamard transforms. Chaotic I and Q scrambling was done in [7] to enhance physical-layer security. Whereas in [8], Brownian motion was studied and implemented to scramble the QAM symbols. In [9], chaotic shuffling of QAM symbols was done using chaotic confusion and diffusion. A recently proposed scheme utilized chaotic frequency for the RF subcarrier [10] in order to encrypt user data. In [11], to provide secure transmission DNA coding rules are applied on user data for encryption and decryption. A joint PAPR reduction and encryption scheme is implemented in [12] by combining the optimal I and Q parts of different QAM symbols. Another recent scheme implemented pilot aided key agreement along with chaotic scrambling of QAM symbols [13] within the constellation, to achieve encryption in physical-layer. However, in all these schemes the target mapping has equi-probable and equi-distant constellation points; therefore, the mapping is fixed, and the QAM symbols are scrambled among the fixed location points of the QAM constellation. Due to the inflexible constellation mapping, the security provided by them is not sufficient. In [14], the target mapping was made dynamic by rotating the constellation points along the radial axis. A similar approach was adopted for physical-layer encryption in wireless communication [15], where chaotic phase rotation was given to QAM symbols. However, this flexibility in mapping QAM symbols still had fixed radial axis, and thus all the schemes user data was vulnerable to attacks due to statistical analysis [16]. Moreover, as the QAM symbols are rotated the Euclidian distance between the constellation points increase; therefore more symbols are required in order to mimic a noise-like constellation. The dynamic mapping of QAM symbols was also considered in [17], where a square QAM was taken, and QAM symbols were mapped dynamically. However, this dynamic mapping was achieved by shifting the constellation, i.e. by increasing the dimensions of a standard QAM constellation. Thereby, a power penalty of 2-dB was incurred due to the increase in dimensions. Therefore, for an efficient encryption scheme, it is desirable that the dynamic mapping of QAM symbols should be achieved with low power penalty.

This paper proposes for the first time a QAM mapping with dynamic radius and phase offsets, to enhance the data encryption in physical-layer during transmission for OFDM-PON. The security is originated by processing each QAM symbol independently with a nonlinear radius and phase mapping, thereby reconstructing a noisy constellation if compared with the conventional QAM mapping. Thus, QAM symbols are distributed over the whole range of constellation, which creates a noisy constellation for the attackers. The improvement in transmission performance, when compared with other dynamic mapping schemes, can be expected, due to the use of radial constellation, where the adjacent constellation points have an increased Euclidean distance and increased angular distance [18]. The transmission experiment is demonstrated for 9.4-Gb/s encrypted OFDM signal transmission over 22-km standard single-mode fiber (SSMF), where the transmission performance is not significantly degraded. A hyper digital chaos is applied for the dynamic mapping of QAM symbol's radius and phase in the constellation, where an overall key space of $\sim 10^{340}$ is created in the proposed multifold security scheme.

II. PRINCIPLE

During the process of dynamic QAM mapping on constellation, the chaotic radius and phase are set independently using chaotic sequences for each QAM symbol. As a result, a fully flexible mapping can be expected, where both the radius and the phase of the original QAM symbol are chaotically offset and appeared randomly on constellation for the purpose of QAM data encryption.

Fig.1 shows the effect of the chaotic mapping, after implementing the chaotic offsets for the radius and the phase, taking an example of 16-QAM. In Fig. 1(a), a standard 16-QAM mapping is shown in which the target mapping is fixed; whereas, in Fig. 1(b), the dynamic mapping of QAM symbols is done, with a chaotic location that is away from the standard location of QAM mapping. For each QAM symbol, the mapping is spread randomly over the entire range of radial constellation. As the offsets of the radius and phase of each QAM symbol are applied independently, it results in a noisy constellation, which provides a multi-fold data encryption.

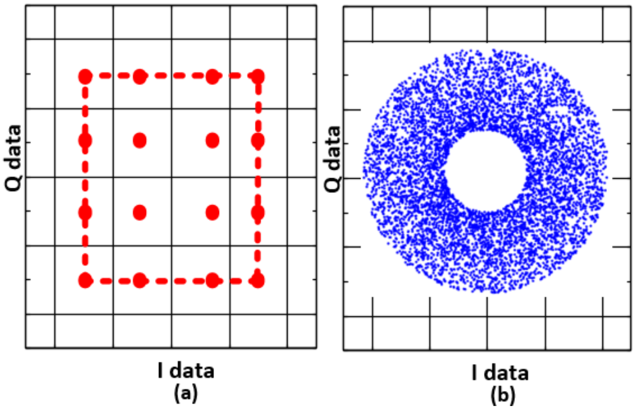


FIGURE 1. Comparison of 16-QAM mapping: (a) Standard QAM; (b) QAM mapping with chaotic radius and phase.

The schematic procedure of dynamic QAM mapping in the proposed scheme is shown in Fig. 2, where the chaotic mapping of radius and phase is determined for an original QAM symbol having position $P_s(r_s, \theta_s)$, where r_s is the radius and θ_s is the angle. A reference chaotic position $P_c(r_c, \theta_c)$ is selected using chaos and the QAM symbol is then mapped at position$P_f(r_f, \theta_f)$, which is selected using chaos and can be anywhere between P_s and P_c.

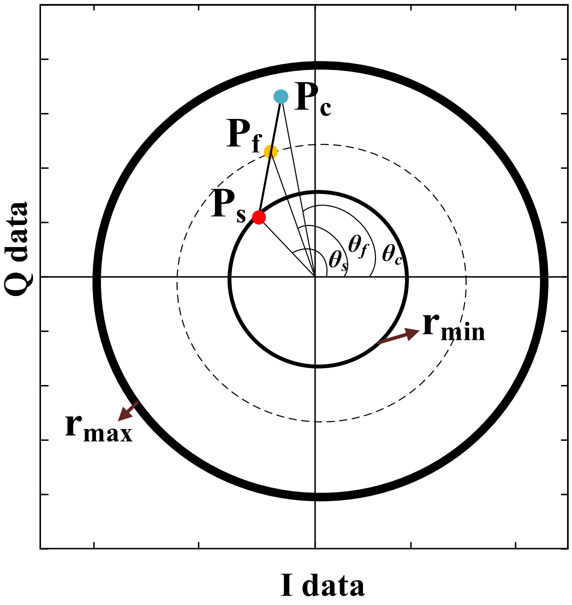


FIGURE 2. Procedure of dynamic QAM mapping.

The offsets applied for the radius and the phase of constellation are obtained via a four-dimensional (4D) hyper digital chaos [19],

$$\begin{cases} \dot{x} = a(-x+y)+yzu \\ \dot{y} = b(x+y)-xzu \\ \dot{z} = cy-u+dxyu \\ \dot{u} = -eu+xyz \end{cases} \tag{1}$$

where *a, b, c, d* and *e* are the real constants, which are used to obtain the independent chaotic sequences $\{x\}$, $\{y\}$, $\{z\}$ and $\{u\}$ respectively, using Runge-kutta method.

The chaotic sequence $\{x\}$ is initially used to determine a chaotic radius, which is confined within the dimensions of the radial QAM,

$$r_c = r_{\max} - (r_{\max} - r_{\min})\,\Delta r \tag{2}$$

where r_{max} and r_{min} are the confined maximum and minimum radii on constellation as shown in Fig. 2, and Δr is a value within (0, 1), which is determined by the chaotic sequence $\{x\}$. The r_c is selected as a reference radius which is set between the maximum and minimum radius rings of the constellation. The angle for the chaotic radius is determined as,

$$\theta_c = 90\,(n-1)+c_p, \quad n = 1, 2, 3, 4 \tag{3}$$

where n is the quadrant in which the original QAM symbol is located, c_p is the angle determined by the chaotic sequence $\{y\}$, and is set to have any value between 0 and 90°.

Using (2) and (3) a reference location within the dimensions of constellation is obtained. Thus, the chaotic point P_c, is determined by,

$$P_c = \underbrace{r_c \cos(\theta_c)}_{I_c} + \underbrace{j r_c \sin(\theta_c)}_{Q_c} \tag{4}$$

Then original QAM symbol having radius r_s is mapped anywhere within the confined dimensions between r_s and r_c. This new location for QAM symbol is obtained as,

$$I_f = (1-d)I_s + I_c d \tag{5}$$

$$Q_f = (1-d)Q_s + Q_c d \tag{6}$$

where d is the chaotic offset of the target position from the original QAM symbol, which is determined by the chaotic sequence of $\{z\}$. The chaotic value of $\{z\}$ is set within (0, 1). Considering Fig. 2, d is the distance between P_s and P_f. After evaluating (5) and (6), the new QAM point has a chaotic radius of

$$r_f = \sqrt{(I_f)^2 + (Q_f)^2} \tag{7}$$

with the chaotic phase of

$$\theta_f = \tan^{-1}(Q_f/I_f) \tag{8}$$

Thus, the location of the encrypted QAM symbol will be offset dynamically with the chaotic radius and phase, as shown in Fig. 2.

However, since the mapping of QAM symbol is dependent on the quadrant in which it is originally located, as defined in (3), the new location of each QAM symbol will be still in the same quadrant as that of original QAM symbol. To eliminate this dependency and to enable QAM symbol mapping in any quadrant, a final phase offset is applied on chaotic point P_f. Therefore, as a next step of multi-fold encryption, the angle θ_f is given a chaotic phase offset θ_t. This offset is determined by the chaotic sequence $\{u\}$, which is set to be anywhere between 0 and 360°. Thus, the final location of QAM symbol can be in any of the quadrant determined by θ_t and θ_f.

Therefore, by using the proposed scheme the new location of the QAM symbol will be given as,

$$P_t = r_f \cos(\theta_f + \theta_t) + j r_f \sin(\theta_f + \theta_t) \tag{9}$$

Due to the chaotic radius and phase mapping of QAM symbols, a final dynamic constellation is constructed. The independent, dynamic mapping of each QAM symbol transfers the original data on a reconstructed constellation that appears severely affected by noise. Thus, the security of user data is significantly enhanced using the proposed secure scheme.

The schematic implementation of the proposed data encryption scheme for OFDM signal generation is shown in Fig. 3, where after serial to parallel conversion (S/P) and standard QAM mapping, the chaotic sequences of $\{x\}$ and $\{y\}$ are used to perform a chaotic row and column permutations as performed in [20]. The row and column permutations are done in order to create randomness in the original QAM symbols. The chaotic radius and phase offsets are then applied on QAM symbols to achieve the proposed multi-fold data encryption. After inverse fast Fourier transform (IFFT), the output data are converted from parallel to serial (P/S) and appended with a cyclic prefix (CP), before sending it into the optical channel.

Since the proposed scheme aims at secure transmission only, therefore, the initial chaotic values that are served as the keys are pre-shared between the legal users. The implementation of Runge-Kutta method requires initial keys to be exchanged for each session. Therefore, it would be spectrally efficient if the secure keys for the next session be shared

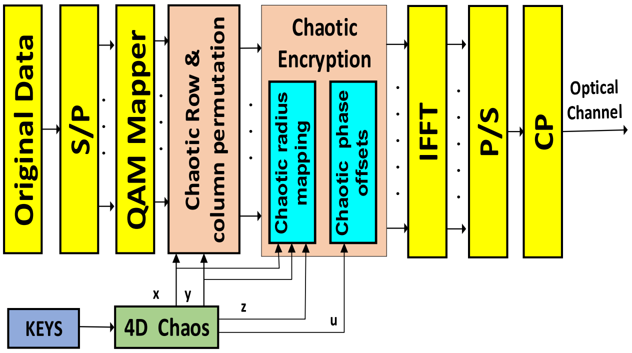


FIGURE 3. Block diagram of the proposed data encryption scheme using QAM mapping with chaotic radius and phase.

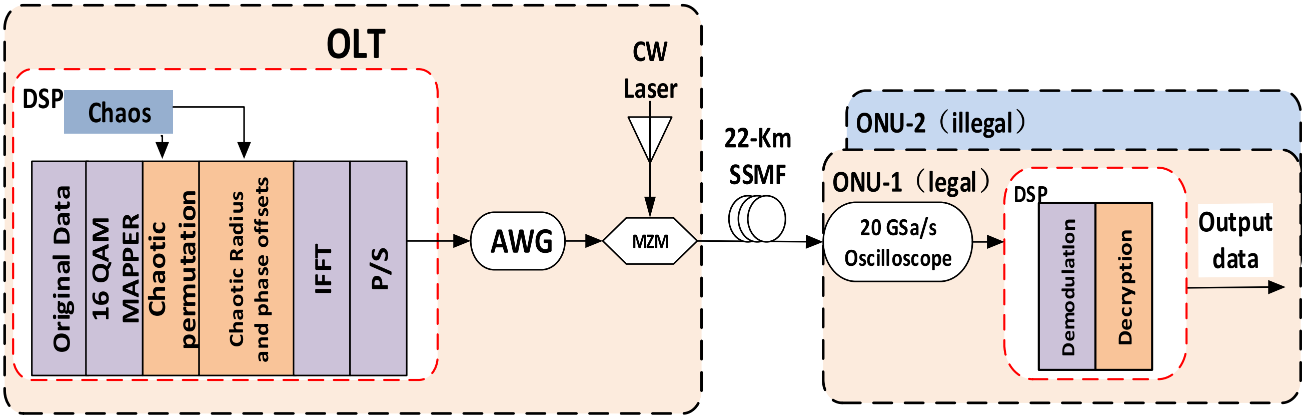


FIGURE 4. Experimental transmission setup of the proposed chaotic QAM encrypted data.

during an ongoing session using [21] and [22]. However, for the first time, before session initiation, the secure keys can be exchanged using [23].With the pre-shared keys, the legal ONU is able to generate the same chaotic sequences as applied at OLT. Then these chaotic sequences are used to decrypt the received OFDM data by removing the applied chaotic radius and phase offsets. However, for an illegal ONU, the received encrypted constellation will reveal no useful information without knowing both the correct offsets as well as the permutation orders. Therefore, the illegal ONU cannot recover original QAM constellation from the received encrypted data due to the lack of shared chaotic keys.

Due to the security offered by the use of 4D hyper digital chaos in the proposed scheme, even with a tiny discrepancy ($\sim 10^{-15}$) from the initial values [24], an illegal ONU will still not be able to recover the correct original data from the received encrypted data. In order to evaluate the robustness of the proposed chaotic encryption scheme, the key space can be estimated as follows. The chaotic row and column permutation creates a key space of $N! \times M!$, where N is the number of QAM symbols and M is the number of OFDM symbols that are to be transmitted. The chaotic radius, chaotic phase of the radius, chaotic distance and the phase offset given to the symbol before transmitting, creates a key space of 10^{15} each. Thus, the total key space of size $N! \times M! \times 10^{15} \times 10^{15} \times 10^{15} \times 10^{15}$ is achieved for the proposed multi-fold chaotic encryption scheme.

III. EXPERIMENT SETUP

To verify the feasibility of the proposed scheme, the experimental setup of the 16-QAM encrypted OFDM data transmission is shown in Fig. 4, where intensity modulation and direct detection (IM/DD) were applied. The 16-QAM data was carried with 256 subcarriers, in which 128 subcarriers were applied as the corresponding complex conjugates for Hermitian symmetry. The IFFT size was 512. A cyclic prefix (CP) of 1/16 length of the OFDM symbol was appended after performing IFFT of the encrypted data and P/S conversion. The data encryption was processed offline by *MATLAB* programs. These encrypted OFDM data were loaded into an arbitrary waveform generator (AWG, Tektronix, 7122C) with a sample rate of 10-GSa/s to generate electrical OFDM signals.

A continuous-wave (CW) laser of the central wavelength at 1550-nm, was used as the optical carrier. The electrical to optical signals conversion was done by a 10-Gb/s optical Mach-Zehnder modulator (MZM), and then transmitted over a 22-km SSMF. At the receiving end, two type of ONUs (ONU-1, ONU-2) were evaluated in the experiment. ONU-1 was the legal ONU; whereas ONU-2 was the illegal ONU, which will receive the same encrypted OFDM signal as ONU-1. A 10-GHz photodiode was used at the ONU side to receive the transmitted optical OFDM signal via direct detection, and then recorded by a 20-Gs/s real-time oscilloscope for offline processing. A net data rate of 9.4-Gb/s was achieved in this experiment. The initial values were pre-shared between OLT and ONUs, and served as the security keys.

IV. RESULTS AND DISCUSSION

The transmission performance of the proposed security scheme is evaluated by bit error ratios (BERs) for 16-QAM OFDM data, as plotted in Fig. 5. BER curves were plotted for the transmission of encrypted OFDM data over 22-km SSMF length, where the back-to-back (b2b) cases for both legal and illegal ONUs are presented as well. The transmitted data were successfully decrypted with the BER $\ll 10^{-3}$ for a legal ONU, with the pre-shared initial keys. Whereas, an illegal ONU could not decrypt the received signal (i.e. BER$\sim$0.5) due to a wrong initial key, which is only a tiny discrepancy ($\sim 10^{-15}$) from the correct initial value.

The corresponding received constellations for the legal and illegal ONUs are shown as the insets in Fig. 5. Even if any blind channel estimation technique is deployed by an illegal ONU, it will not be able to map it back to a standard 16-QAM constellation. Therefore, providing flexibility in mapping QAM symbols chaotically on dynamic radius will

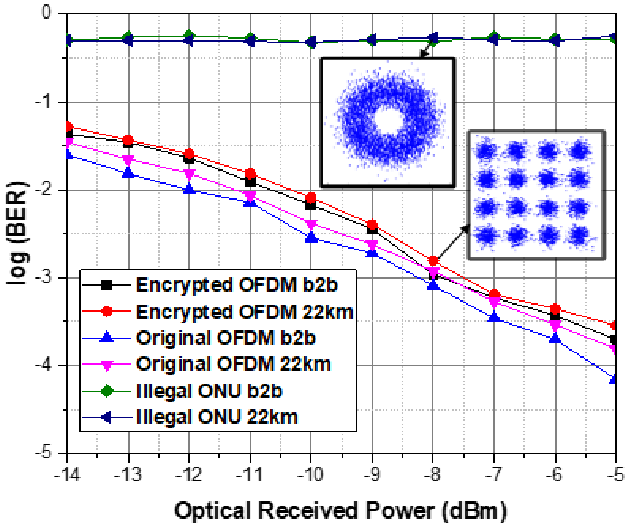


FIGURE 5. BER performance of the proposed scheme.

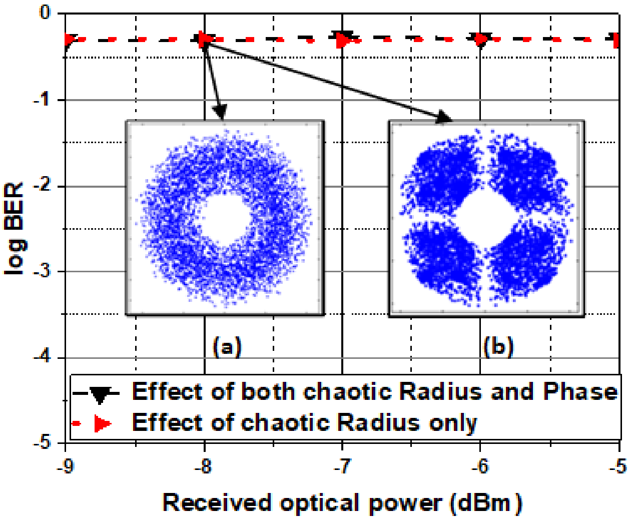


FIGURE 6. BER and constellations: (a) with chaotic radius and phase offsets; (b) with chaotic radius offset only.

scramble the data in such a way that it appears as a noisy constellation that reveals no information about the original mapping to an illegal ONU.

To verify the effect of the proposed encryption scheme on transmission performance, the BER analysis of an unencrypted standard 16-QAM OFDM signal is also plotted for comparison in Fig. 5. A power penalty of ~0.25-dB was incurred for the encrypted 16-QAM OFDM data, if it is compared with the unencrypted 16-QAM OFDM data. While encrypting only the phase of QAM symbol, would increase the Euclidean distance between the constellation points, which eventually would result in a gain as compared to unencrypted 16-QAM OFDM data [25].

For evaluating the effectiveness of the proposed dynamic radius mapping, the BER with the corresponding encrypted constellations are shown in Fig. 6, for the b2b signals received by an illegal ONU. In Fig. 6(a), the constellation is shown for

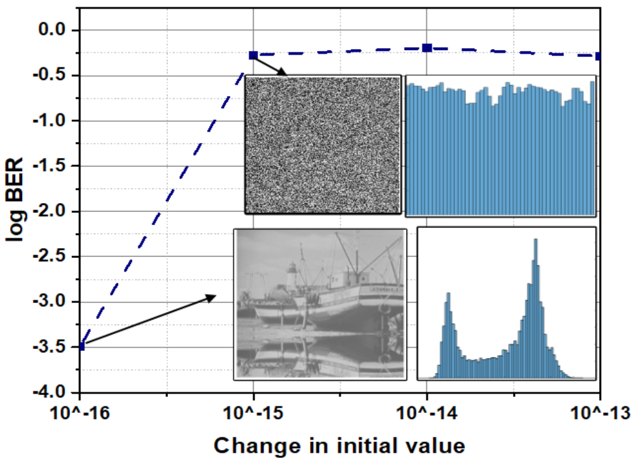


FIGURE 7. BER performance with respect to the change in initial value.

the case after applying the chaotic radius and phase offsets. It can be seen that, the constellation appears as severely affected by offsets and does not reveal any information to an illegal ONU at any optical received power. In Fig. 6(b), the effect is shown for the case of applying only the chaotic radius mapping. It can be seen that, due to the dynamic radius mapping, the distribution of constellation points along the fixed radial axis, as employed by giving only phase offset, is destroyed. However, as the mapping caused due to only chaotic phase or only chaotic radius is dimension constrained, the security offered by them alone is limited. Therefore, to make the mapping fully dynamic and to destroy the statistics of QAM constellation, both chaotic phase and radius mapping are recommended. It can be seen from Fig. 6(a), that the constellation does not reveal any statistical information about QAM symbols, which reveals a clear evidence of significant enhancement in security.

The high-level security in the proposed encryption scheme can be analyzed via the sensitivity of digital chaotic sequences to the chaotic initial values. To illustrate clearly the sensitivity in the proposed encryption scheme, the data encryption is performed for the input data—a digital image. The BERs are calculated and shown in Fig. 7 with the correct the correct initial values and a tiny deviation ($\sim 10^{-15}$) from it. It can be noted that, with the small deviation from the initial values, the received images will not be correctly recovered as entirely different chaotic sequence is obtained. Therefore, the tiny deviation in the initial value results in significant degradation of BER ($\gg 10^{-3}$), which is far above the threshold required for forward error correction (FEC). This implies that it is impossible to decrypt the correct original image with even a tiny deviation from the correct initial values. Moreover, the corresponding histograms of the image are plotted as the insets in Fig. 7, where there is a good uniformity in the histogram of the encrypted image, which also reveals that the good security performance is achieved, due to that the statistics in the original image is successfully destroyed after using chaotic data encryption.

Finally, the robustness of security performance for the proposed encryption scheme can be quantitatively evaluated via the key space to resist any exhaustive attacks. First, the row and column permutation creates a key space of $50! \times 128!$; second, the independent chaotic sequences for phase offset θ_t, dynamic radius r_c, the angle of the radius θ_c and the chaotic distance d at which the new QAM symbol is located, creates an additional key space of $10^{15} \times 10^{15} \times 10^{15} \times 10^{15}$. Therefore, the total key space of the chaotic radius mapping encryption scheme is $\sim 10^{340}$ (i.e., $10^{15} \times 10^{15} \times 10^{15} \times 10^{15} \times 50! \times 128!$), which provides strong security against any brute-force attacks. Moreover, the scheme uses independent chaotic sequences for encryption of the phase and radius; therefore extracting the secure keys from the received signal will be extremely difficult for attackers.

V. CONCLUSION

Chaotic radius encryption is proposed and demonstrated for the dynamic mapping in QAM constellation to enhance physical-layer security during OFDM data transmission. In the proposed scheme, QAM symbols are independently and flexibly distributed on the complex plane, with chaotic radius of the rings and chaotic phase offsets, which leads to noise-like constellation. The robustness of the security provided by the proposed encryption scheme is evaluated, where a total key space of $\sim 10^{340}$ is provided. Successful encrypted data transmission of 9.4-Gb/s is accomplished for a legal ONU, where the power penalty is as small as ~0.25-dB for the encrypted OFDM signals, if compared with the standard QAM OFDM signals. Both experimental and analytical results show that the proposed scheme can be a good candidate for next-generation secure OFDM-PON.

REFERENCES

[1] J.-I. Kani *et al.*, "Next-generation PON-Part I: Technology roadmap and general requirements," *IEEE Commun. Mag.*, vol. 47, no. 11, pp. 43–49, Nov. 2009.

[2] N. Cvijetic, "OFDM for next-generation optical access networks," *J. Lightw. Technol.*, vol. 30, no. 4, pp. 384–398, Feb. 15, 2012.

[3] 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.

[4] A. Argyris, E. Grivas, M. Hamacher, A. Bogris, and D. Syvridis, "Chaos-on-a-chip secures data transmission in optical fiber links," *Opt. Express*, vol. 18, no. 5, pp. 5188–5198, Feb. 2010.

[5] M. van Turnhout and F. Bociort, "Chaotic behavior in an algorithm to escape from poor local minima in lens design," *Opt. Express*, vol. 17, no. 8, pp. 6436–6450, 2009.

[6] A. A. E. Hajomer, X. Yang, and W. Hu, "Chaotic Walsh–Hadamard transform for physical layer security in OFDM-PON," *IEEE Photon. Technol. Lett.*, vol. 29, no. 6, pp. 527–530, Mar. 15, 2017.

[7] W. Zhang, C. F. Zhang, W. Jin, C. Chen, N. Jiang, and K. Qiu, "Chaos coding-based QAM IQ-encryption for improved security in OFDMA-PON," *IEEE Photon. Technol. Lett.*, vol. 26, no. 19, pp. 1964–1967, Oct. 1, 2014.

[8] W. Zhang, C. Zhang, C. Chen, H. Zhang, and K. Qiu, "Brownian motion encryption for physical-layer security improvement in CO-OFDM-PON," *IEEE Photon. Technol. Lett.*, vol. 29, no. 12, pp. 1023–1026, Jun. 15, 2017.

[9] W. Zhang, C. Zhang, C. Chen, H. Zhang, W. Jin, and K. Qiu, "Hybrid chaotic confusion and diffusion for physical layer security in OFDM-PON," *IEEE Photon. J*, vol. 9, no. 2, Apr. 2017, Art. no. 7201010.

[10] 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.

[11] 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. 1706–1712, May 1, 2018.

[12] W. Zhang, C. Zhang, C. Chen, W. Jin, and K. Qiu, "Joint PAPR reduction and physical layer security enhancement in OFDMA-PON," *IEEE Photon. Technol. Lett.*, vol. 28, no. 9, pp. 998–1001, May 1, 2016.

[13] 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 1, 2017.

[14] B. Liu, L. Zhang, X. Xin, and J. Yu, "Constellation-masked secure communication technique for OFDM-PON," *Opt. Express*, vol. 20, no. 22, pp. 25161–25168, 2012.

[15] T. Liang, K. Wang, C. Lim, E. Wong, T. Song, and A. Nirmalathas, "Secure multiple access for indoor optical wireless communications with time-slot coding and chaotic phase," *Opt. Express*, vol. 25, no. 18, pp. 22046–22054, 2017.

[16] Q. Chen *et al.*, "Security scheme in IMDD-OFDM-PON system with the chaotic pilot interval and scrambling," *Opt. Commun.*, vol. 407, no. 1, pp. 285–289, 2018.

[17] 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. 339–342, Feb. 15, 2018.

[18] M. N. Khormuji, U. H. Rizvi, G. J. M. Janssen, and S. B. Slimane, "Rotation optimization for MPSK/MQAM signal constellations over Rayleigh fading channels," in *Proc. 10th IEEE Singapore Int. Conf. Commun. Syst.*, Oct./Nov. 2006, pp. 1–5.

[19] M. Cheng *et al.*, "Security-enhanced OFDM-PON using hybrid chaotic system," *IEEE Photon. Technol. Lett.*, vol. 27, no. 3, pp. 326–329, Feb. 1, 2015.

[20] X. Yang, Z. Shen, X. Hu, and W. Hu, "Chaotic encryption algorithm against chosen-plaintext attacks in optical OFDM transmission," *IEEE Photon. Technol. Lett.*, vol. 28, no. 22, pp. 2499–2502, Nov. 15, 2016.

[21] 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.

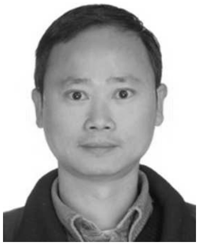
[22] S. Li *et al.*, "Secure key distribution strategy in OFDM-PON by utilizing the redundancy of training symbol and digital chaos technique," *IEEE Photon. J.*, vol. 10, no. 2, Apr. 2018, Art. no. 7201108.

[23] A. A. E. Hajomer, X. Yang, A. Sultan, and W. Hu, "Key distribution based on phase fluctuation between polarization modes in optical channel," *IEEE Photon. Technol. Lett.*, vol. 30, no. 8, pp. 704–707, Apr. 15, 2018.

[24] X. Hu, X. Yang, Z. Shen, H. He, W. Hu, and C. Bai, "Chaos-based partial transmit sequence technique for physical layer security in OFDM-PON," *IEEE Photon. Technol. Lett.*, vol. 27, no. 23, pp. 2429–2432, Dec. 1, 2015.

[25] A. Sultan, X. Yang, S. B. Hussain, and W. Hu, "Chaotic radial constellation rotation for physical-layer security in OFDM-PON," in *Proc. Asia Commun. Photon. Conf., Opt. Soc. Amer.*, 2017, Paper Su1C-1.

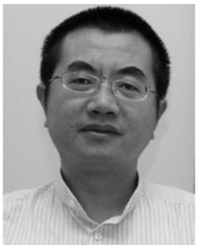
AMBER SULTAN received the M.Sc. degree in telecommunication engineering from National University FAST, Pakistan, in 2008. She is currently pursuing the Ph.D. degree with the State Key Laboratory of Advanced Optical Communication Systems and Networks, Shanghai Jiao Tong University. Her research interest mainly focuses on data encryption based on digital chaos.



XUELIN YANG is currently a Professor with Shanghai Jiao Tong University. His interests mainly focused on ultrafast all-optical signal processing in optical fiber communication, applications of semiconductor optical amplifiers, security of optical networks, optical orthogonal frequency-division multiplexing transmission, and passive optical networks.

ADNAN A. E. HAJOMER received the M.Sc. degree in telecommunication engineering from Shanghai Jiao Tong University in 2017, where he is currently pursuing the Ph.D. degree with the State Key Laboratory of Advanced Optical Communication Systems and Networks. His research interest mainly focuses on optical orthogonal frequency-division multiplexing transmission and passive optical networks.

SYED B. HUSSAIN received the Ph.D. degree in telecommunication engineering from Shanghai Jiao Tong University in 2018.



WEISHENG HU is currently a Professor with Shanghai Jiao Tong University. He serves on the Editorial Board of *Optics Express*, the *Journal of Lightwave Technology*, and *Chinese Optics Letters*.