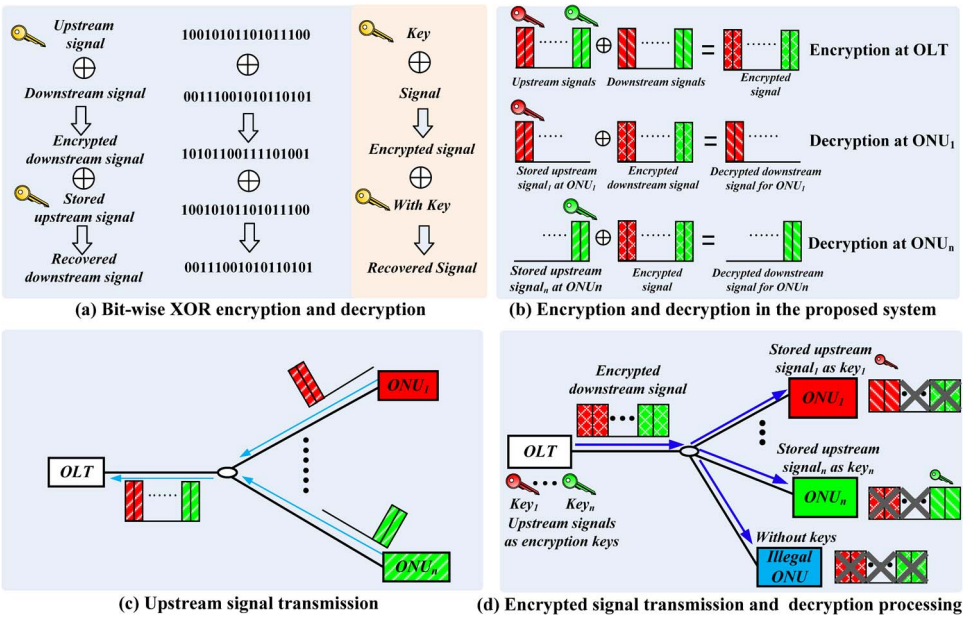
IEEE Photonics Journal
An IEEE Photonics Society Publication

Open Access

Physical Layer Encryption in OFDM-PON Employing Time-Variable Keys From ONUs

Volume 6, Number 2, April 2014

Pan Cao
Xiaofeng Hu
Jiayang Wu
Liang Zhang
Xinhong Jiang
Yikai Su, Senior Member, IEEE



(a) Bit-wise XOR encryption and decryption

(b) Encryption and decryption in the proposed system

(c) Upstream signal transmission

(d) Encrypted signal transmission and decryption processing

DOI: 10.1109/JPHOT.2014.2311451
1943-0655 © 2014 IEEE

Physical Layer Encryption in OFDM-PON Employing Time-Variable Keys From ONUs

Pan Cao, Xiaofeng Hu, Jiayang Wu, Liang Zhang, Xinhong Jiang, and Yikai Su, *Senior Member, IEEE*

State Key Laboratory of Advanced Optical Communication Systems and Networks, Department of Electronic Engineering, Shanghai Jiao Tong University, Shanghai 200240, China

DOI: 10.1109/JPHOT.2014.2311451
1943-0655 © 2014 IEEE. Translations and content mining are permitted for academic research only. Personal use is also permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.

Manuscript received January 25, 2014; revised March 3, 2014; accepted March 4, 2014. Date of current version March 20, 2014. This work was supported in part by the National Natural Science Foundation of China under Grant 61125504, by the 863 High-Tech Program under Grant 2013AA013402, and by Minhang Talent Program. Corresponding author: Y. Su (e-mail: yikaisu@sjtu.edu.cn).

Abstract: We propose and experimentally demonstrate a dynamic encryption method to realize physical layer security for orthogonal frequency division multiplexing passive optical network (OFDM-PON). In our scheme, encryption of the downstream signal is obtained by applying exclusive or (XOR) operation between optical network units' (ONUs') downstream signals and received upstream signals at the optical line terminal side. The upstream signals are used as secure keys for corresponding ONUs. Then the encrypted downstream signals are sent to the ONU sides, where the downstream signal can be retrieved by applying XOR operation again between the encrypted downstream signal and the stored upstream signal. Since each ONU cannot obtain the upstream signals of other ONUs, only the ONU itself can recover its downstream signal from the encrypted downstream signal. Moreover, the secure key is dynamically changing along with the upstream signal, significantly improving the security of the downstream signal for the OFDM-PON system. A 5-Gb/s 16-quadrature amplitude modulation OFDM signal with XOR-based encryption has been successfully implemented over a 25-km standard single-mode fiber. Experimental results verify that the encryption scheme can effectively prevent eavesdropping by malicious users.

Index Terms: Orthogonal frequency division multiple (OFDM), passive optical network (PON), physical layer encryption.

1. Introduction

Driven by the ever-increasing data traffic of multimedia services, the bandwidth requirement is fast growing in optical access networks [1], [2]. Orthogonal frequency division multiplexing passive optical network (OFDM-PON) has been regarded as a promising candidate for next-generation optical access network owing to its high spectral efficiency and resistance to chromatic dispersion (CD) [3]. Because of the broadcast nature of OFDM-PON in the downstream direction, each optical network unit (ONU) can receive other ONUs' downstream signals. In practical networks, e-bank accounts, credit card information, and financial transactions may be eavesdropped by malicious users [4]. Therefore, security of the downstream signal has become an important issue in OFDM-PONs.

MAC-layer encryptions have been reported to improve the security of PON system [5], [6]. However, in these schemes, the control signals may be not effectively protected as indicated in [7], [8]. Physical layer encryption has been proposed to further improve the security of downstream transmission in optical access networks, which is a transparent encryption scheme for different data

types [9]. Thanks to the convenient digital signal processing (DSP) of OFDM signal, the downstream signal encryptions have been realized at the physical layer by using different methods, including constellation masking, chaos scrambling, and chaotic permutation [10]–[12]. Then the encrypted downstream signals are transmitted to the ONU sides, where the downstream signals can be decrypted by using the corresponding key. However, due to the broadcast nature of OFDM-PON system, the ONU's downstream signal still has potential risk of being eavesdropped by malicious users once they have the secure key.

In this paper, we propose and experimentally demonstrate a dynamic security method for physical layer encryption in OFDM-PON. The upstream signals from each ONU are received at the optical line terminal (OLT) side, and the encryption is obtained by bit-wise exclusive or (XOR) operation between ONU's downstream and upstream signals. Here, each ONU's upstream signal is used as its secure key. The encrypted downstream signals are sent to the ONU sides, where each ONU selects its own OFDM subcarriers. Then the decryption processing is realized by using XOR operation between the encrypted downstream signal and the stored upstream signal. Therefore, only ONU itself can decrypt the encryption signal because it has a copy of its upstream signal. Since DSP is easy to be implemented in OFDM-PON system and ONU cannot obtain other ONUs' upstream signals, XOR between downstream and upstream signals is a simple and effective encryption method for downstream signal. Moreover, the upstream signal of each ONU is time-varying, implying that the secure key is dynamically changing. A proof-of-concept experiment is performed to verify the feasibility of our proposal. Successful transmission of 5-Gb/s 16-quadrature amplitude modulation (QAM) OFDM encrypted downstream signal has been demonstrated over a 25-km standard single mode fiber (SSMF). Experimental results validate that the proposed encryption scheme can greatly enhance the security of OFMD-PON system.

2. Operation Principle

2a. Basic Principle

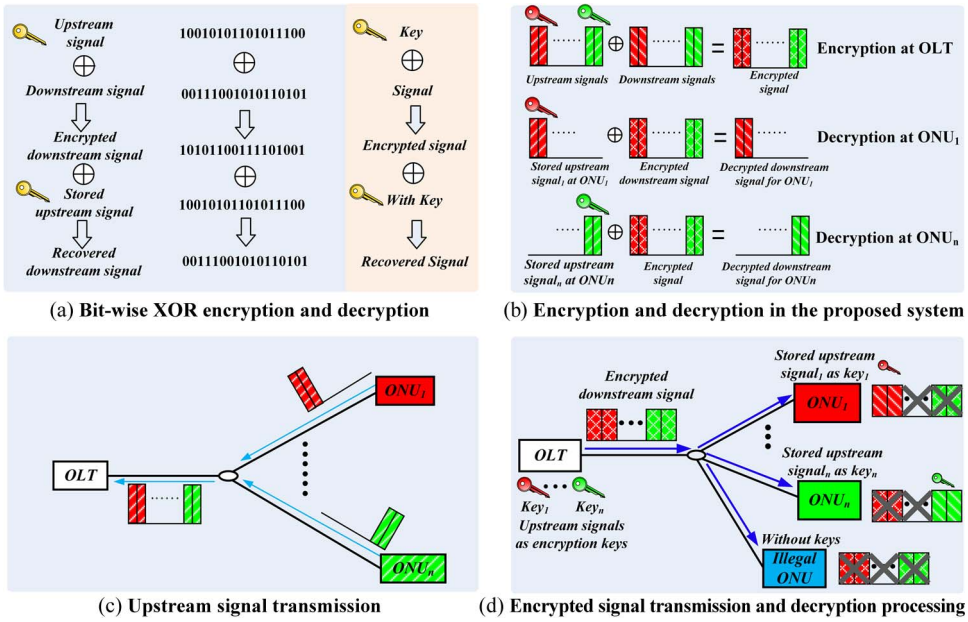
Fig. 1(a) illustrates the principle of bit-wise XOR encryption and decryption. Each ONU's upstream signal is used as its secure key in our proposed method. The downstream signal encryption is realized by employing XOR operation between upstream and downstream signals. Then the encrypted downstream signal can be decrypted by applying XOR operation with the stored upstream signal at each ONU. The principles of encryption at OLT, decryption at ONU_1 and ONU_n are depicted in Fig. 1(b), where only ONU itself can decrypt the encrypted downstream signal. As shown in Fig. 1(c), the upstream data from each ONU are modulated onto different optical carriers and transmitted to the OLT side. Fig. 1(d) describes the encrypted downstream signal transmission and decryption processing at the ONU sides. One ONU cannot decrypt other ONUs' downstream signals due to the lack of their upstream signals. Thus the downstream signal security is guaranteed by using XOR operation. Moreover, the secure key is dynamically changing with the upstream signal. Therefore, the physical layer security can be greatly improved via the proposed method.

2b. Asymmetric Transmission Scenario and Storage Time of Upstream Signal in the Proposed Encryption System

In this paper, the downstream signal encryption is achieved by applying XOR operation between ONU's downstream and upstream signals at the OLT side. However, the bit-rates of upstream and downstream signals are usually different, resulting in asymmetric transmission for the PON system. Generally speaking, the bit-rate of the downstream signal is higher than that of the upstream signal [2]. We define an asymmetry parameter A (a positive integer), which satisfies the inequality

$$(A-1)It;(R_d/R_u) \leq A \tag{1}$$

where R_d and R_u are the bit-rates of downstream and upstream signals, respectively. We can repeat the upstream signal A times and then apply encryption and decryption processing.



(a) **Bit-wise XOR encryption and decryption** (b) **Encryption and decryption in the proposed system**

(c) **Upstream signal transmission** (d) **Encrypted signal transmission and decryption processing**

Fig. 1. (a) Principle of bit-wise XOR encryption and decryption. (b) Schematic diagrams of encryption at OLT, decryption at ONU_1 and ONU_n. (c) Upstream transmission of the proposed OFDM-PON system. (d) Encrypted downstream signal transmission and decryption processing at different ONU sides.

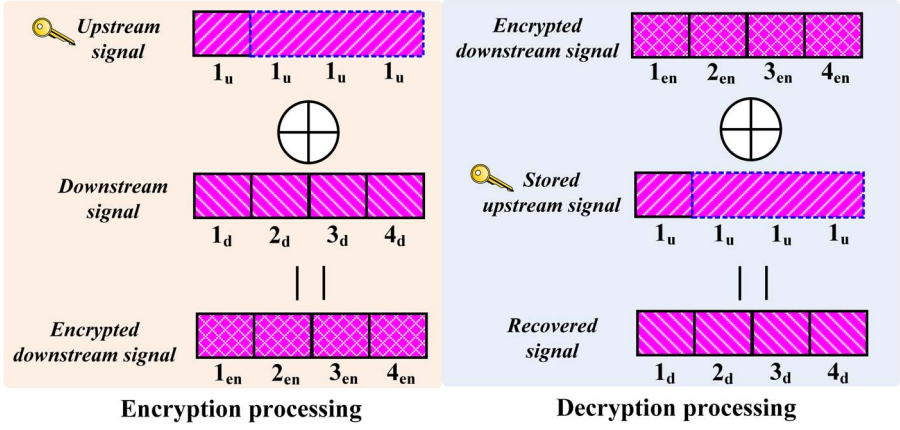


Fig. 2. Principle of bit-wise XOR encryption and decryption processing under asymmetry transmission scenario.

It is known that 4 : 1 asymmetry is a common scenario in the optical access network [3]. Fig. 2 illustrates the principle of bit-wise XOR encryption and decryption processing when the asymmetry parameter is 4. When the bit rate of the upstream signal is lower, the asymmetry parameter can be increased to deal with it. If the bit-rate of the downstream signal is lower than the upstream signal, the encryption processing can be realized by applying XOR operation between the downstream signal and part of the upstream signal. When the upstream transmitter is idle, the OLT can store a previous frame as security key for the ONU. The secure key can be updated until there is upstream signal. Here, the minimum granularity of XOR operation is an OFDM frame. OLT and ONU can respectively realize encryption and decryption operations when the frame synchronization is obtained. Note that the asymmetry parameters are different for ONUs and changing along with the real-time traffics.

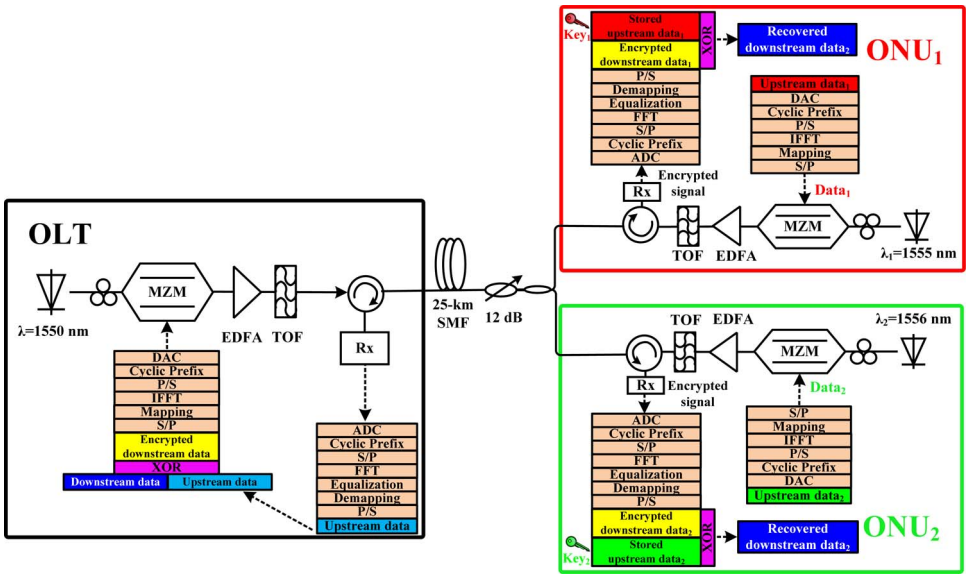


Fig. 3. Experimental setup of XOR-based encryption in OFDM-PON system.

In a conventional PON system, the upstream signals can be temporarily stored at the ONU sides [13], [14]. For the proposed OFDM-PON, the upstream signal needs to be stored at the ONU side to decrypt the encrypted downstream signal. The storage time is the same as the round trip delay of each ONU. For a PON system with 25-km feeder fiber, it contributes 250 μs to the round trip delay [15]. Therefore, the upstream signals need to be restored for 250 μs at the ONU sides. We assume that a 40-Gb/s PON system has 32 users and each ONU has 25-km fiber length. When each ONU has the same upstream bit rate, the additional memory for upstream storage can be calculated by $40/32 \times 250 \times 10^{-6}$ Gb $= 0.32$ Mb. It should be noted that ONUs with different distribution fiber lengths require different storage times [16].

3. Experimental Setup and Results

A proof-of-concept experimental setup for XOR-based encryption in OFDM-PON system is depicted in Fig. 3. In our experiment, the OFDM signal is generated offline by MATLAB, and the IFFT size is 1024. A frequency guard band equal to the signal bandwidth is used to separate the OFDM signal from the optical carrier. Intensity modulation-direct detection (IM-DD) OFDM signal is obtained by using Hermitian symmetry before the IFFT [17]. Therefore, 256 subcarriers are filled with the OFDM signal. The DSPs at the OLT and ONU sides are illustrated in Fig. 3. Meanwhile, a training sequence is inserted to realize timing synchronization and channel equalization [18]. Data_1 and Data_2 for ONU_1 and ONU_2 are output by an arbitrary waveform generator (Tektronix 7122C) with 5-GSample/s sampling rate and 10-bit resolution of digital-to-analog conversion (DAC). It is assumed that each ONU has 64 subcarriers and 4 subcarriers are set to be zero as guard band. Then each ONU has a raw bit-rate of 1.25 Gb/s when each subcarrier uses 16-QAM format. The electrical spectra of the two signals are presented in Fig. 4(a) and (b). For the upstream transmissions, two continuous wave (CW) lights from distributed feedback (DFB) lasers with wavelengths at $\lambda_1 = 1555$ nm and $\lambda_2 = 1556$ nm are fed into two 10-GHz single-drive Mach–Zehnder modulators (MZMs) at ONU_1 and ONU_2 sides, respectively. Polarization controllers (PCs) are employed to obtain good performances, and the two MZMs are both biased at the quadrature points. The output signal of each MZM is amplified by an erbium doped fiber amplifier (EDFA), and a tunable optical filter (TOF) is used to suppress the amplified spontaneous emission (ASE) noise. Then the two upstream signals are combined together by a 3-dB optical coupler. At the remote node (RN), a 12-dB optical attenuator is used to emulate a 1 : 16 optical splitter.

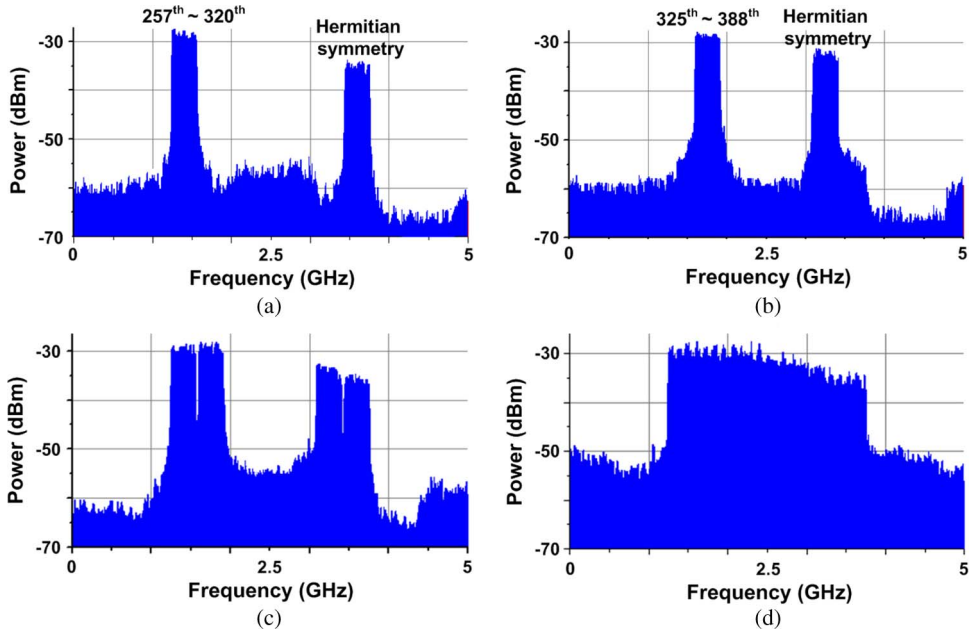


Fig. 4. (a) Electrical spectrum of OFDM $Data_1$ at ONU_1. (b) Electrical spectrum of OFDM $Data_2$ at ONU_2. (c) Electrical spectrum of combined upstream OFDM data at the OLT. (d) Electrical spectrum of the encrypted downstream OFDM signal.

After 25-km SSMF transmission, at the OLT side, the upstream OFDM signals from the two ONUs are detected by a photo detector (PD). The electrical spectrum of the combined signal is shown in Fig. 4(c). After sampled by a real-time oscilloscope (Tektronix DSA70804) and off-line DSP, the upstream signals can be recovered at the OLT side. We assume that the raw bit-rates of downstream signals for ONU_1 and ONU_2 are 1.25 Gb/s and 3.75 Gb/s, respectively. Since the upstream bit-rates of the two ONUs are both 1.25 Gb/s, the asymmetry parameters for ONU_1 and ONU_2 are 1 and 3, respectively. As described in Figs. 2 and 3, the encryption processing of ONU_1 can be realized by applying XOR operation between ONU_1's downstream and upstream signals. For ONU_2, the upstream signal repeats 3 times, and then applying XOR operation with its downstream signal. Fig. 4(d) depicts the electrical spectrum of the encrypted downstream signal. A CW light at $\lambda = 1550$ nm is fed into a single-drive MZM and modulated by the encrypted OFDM signal. Then the encrypted downstream signals are transmitted to the ONU sides, and an ONU can only recover its own downstream signal since it has the stored upstream signal.

Fig. 5 depicts the bit error ratio (BER) performances of the upstream signals and decrypted downstream signals in the proposed OFDM-PON system. At forward error correction (FEC) threshold of 1×10^{-3}, the receiver sensitivities of ONU_1's upstream signal, ONU_2's upstream signal, decrypted downstream signals at ONU_1 and ONU_2 are -20.4 dBm, -20.2 dBm, -19.6 dBm, and -19.2 dBm, respectively. The decrypted downstream signals have worse BER performances than the upstream signals because the transmission errors of upstream signals can affect the encrypted downstream signals. For the illegal and mismatched ONUs, the BERs are 0.5, which verify that our proposed scheme is a reliable security method. It is worth noting that the proposed encryption concept can also be used in other PONs with broadcast nature.

4. Conclusion

We have demonstrated a dynamic encryption scheme to realize physical layer encryption for OFDM-PON system based on XOR operation. The upstream signals from ONUs are used as secure keys of their corresponding downstream signals, and the encryption processing is achieved by applying XOR operation between ONU's downstream and upstream signals. The method

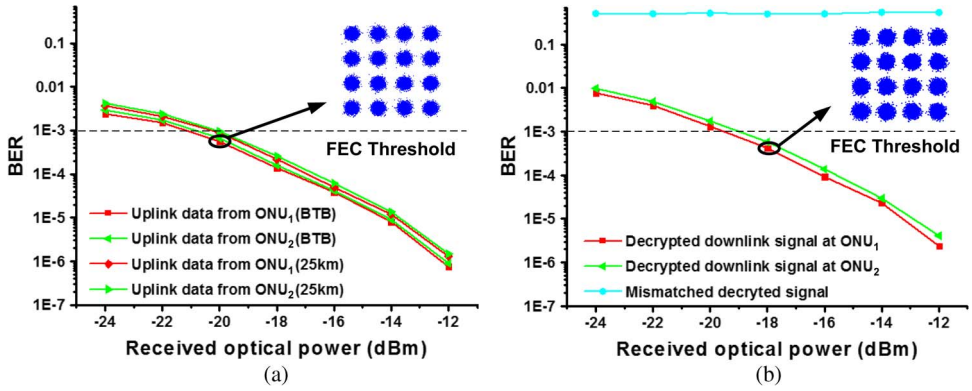


Fig. 5. (a) BER curves of upstream OFDM signals. (b) BER curves of decrypted downlink signals at ONU_1, ONU_2, and mismatched ONUs.

effectively improves the security since only ONU itself can decrypt the encrypted downstream signal. 5-Gb/s OFDM signal with XOR-based encryption has been implemented to verify our proposal. Experimental results show that the proposed security method can effectively prevent eavesdropping by other users.

References

[1] J. Kani, F. Bourgart, A. Cui, A. Rafel, M. Campbell, R. Davey, and S. Rodrigues, "Next-generation PON—Part I: Technology roadmap and general requirements," *IEEE Commun. Mag.*, vol. 47, no. 11, pp. 43–49, Nov. 2009.
[2] F. J. Effenberger, H. Mukai, S. Park, and T. Pfeiffer, "Next-generation PON—Part II: Candidate systems for next-generation PON," *IEEE Commun. Mag.*, vol. 47, no. 11, pp. 50–57, Nov. 2009.
[3] N. Cvijetic, "OFDM for next-generation optical access networks," *J. Lightw. Technol.*, vol. 30, no. 4, pp. 384–398, Feb. 2012.
[4] K. Kitayama, M. Sasaki, S. Araki, M. Tsubokawa, A. Tomita, K. Inoue, K. Harasawa, Y. Nagasako, and A. Takada, "Security in photonic networks: Threats and security enhancement," *J. Lightw. Technol.*, vol. 29, no. 21, pp. 3210–3222, Nov. 2011.
[5] A. Harris, D. R. Jones, K. H. Horbatuck, and A. Sierra, "A novel wavelength hopping passive optical network (WH-PON) for provision of enhanced physical security," *J. Opt. Comm. Netw.*, vol. 4, no. 3, pp. 289–295, Feb. 2012.
[6] S. S. Roh and S.-H. Kim, "Security model and authentication protocol in EPON-based optical access network," in *Proc. 5th Int. Conf. Transparent Optical Networks*, 2003, pp. 99–102.
[7] S. Etemad, A. Agarwal, T. Banwell, G. D. Crescenzo, J. Jackel, R. Menendez, and P. Toliver, "An overlay photonic layer security approach scalable to 100 Gb/s," *IEEE Commun. Mag.*, vol. 46, no. 8, pp. 32–39, Aug. 2008.
[8] G. Cincotti, V. Sacchieri, G. Manzacca, N. Kataoka, N. Wada, N. Nakagawa, and K. Kitayama, "Physical layer security: All-optical cryptography in access networks," presented at the Proc. ICTON, Athens, Greece, 2008, We.A4.2.
[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] 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, Jul. 2011.
[11] B. Liu, L. Zhang, X. Xin, and J. Yu, "Constellation-masked secure communication technique for OFDM-PON," *Opt. Express*, vol. 20, no. 22, pp. 25 161–25 168, Oct. 2012.
[12] B. Liu, L. Zhang, X. Xin, and Y. Wang, "Physical layer security in OFDM-PON based on dimension-transformed chaotic permutation," *IEEE Photon. Technol. Lett.*, vol. 26, no. 2, pp. 127–130, Jan. 2014.
[13] G. Kramer, B. Mukherjee, S. Dixit, Y. Ye, and R. Hirth, "Supporting differentiated classes of service in Ethernet passive optical networks," *J. Opt. Netw.*, vol. 1, no. 8, pp. 280–298, Aug. 2002.
[14] F. T. An, K. S. Kim, D. Gutierrez, S. Yam, E. Hu, K. Shrikhande, and L. G. Kazovsky, "SUCCESS: A next-generation hybrid WDM/TDM optical access network architecture," *J. Lightw. Technol.*, vol. 22, no. 11, pp. 2557–2569, Nov. 2004.
[15] R. P. Davey, P. Healey, I. Hope, P. Watkinson, D. B. Payne, O. Marmur, J. Ruhmann, and Y. Zuiderveld, "DWDM reach extension of a GPON to 135 km," *J. Lightw. Technol.*, vol. 24, no. 1, pp. 29–31, Jan. 2006.
[16] ITU-T G. 987.1, Series G: Transmission systems and media, digital systems and networks. Digital sections and digital line system-Optical line systems for local and access networks" 2010.
[17] R. P. Giddings, X. Q. Jin, E. Hugues-Salas, E. Giacoumidis, J. L. Wei, and J. M. Tang, "Experimental demonstration of a record high 11.25 Gb/s real-time optical OFDM transceiver supporting 25 km SMF end-to-end transmission in simple IMDD systems," *Opt. Express*, vol. 18, no. 6, pp. 5541–5555, Mar. 2010.
[18] D. Qian, N. Cvijetic, J. Hu, and T. Wang, "A novel OFDMA-PON architecture with source-free ONUs for next-generation optical access networks," *IEEE Photon. Technol. Lett.*, vol. 21, no. 17, pp. 1265–1267, Sep. 2009.