Intrinsic Interference Based Physical Layer Encryption for OFDM/OQAM

Manabu Sakai, *Student Member, IEEE,* Hai Lin, *Senior Member, IEEE,* and Katsumi Yamashita, *Member, IEEE*

***Abstract*—A physical layer encryption method is proposed for orthogonal frequency division multiplexing with offset quadrature amplitude modulation. The proposed method uses intentionally added pure imaginary symbols as keys so that their intrinsic interferences can obfuscate true data symbols at the eavesdroppers. The key generation method and four loading patterns are proposed. Also, the impact of channel estimation error, the robustness against ciphertext attacks, and the information leakage at the eavesdropper are analyzed. Finally, the performance of the proposed method is evaluated through numerical simulations.**

***Index Terms*—OFDM/OQAM, Physical Layer Encryption.**

I. Introduction

Confidentiality is a fundamental problem in wireless communications since anyone within the cover area of the transmitter can listen the transmitted signal and has a potential to demodulate then decode it maliciously [1]. The increasing demands for secure wireless communications have largely driven the research of physical layer security (PLS). A lot of PLS methods have been proposed to improve secure capacity [2], [3], for example, artificial noise injection [4] and multiple-input and multiple-output beamforming [5]. However, these methods require multiple transmit antennas or amplifying relays, which increases implementation complexity.

In contrast to PLS schemes which achieve information-theoretic security by exploiting channel characteristics, physical layer encryption (PLE) directly encrypts the transmitted signal [6]. In the literature, there are several PLE methods proposed for orthogonal frequency division multiplexing (OFDM) systems [6]–[11]. The encryption by modifying in-phase and quadrature parts of the data symbols is proposed in [7], while the pseudo random constellation rotation is employed with weak artificial noise in [8]. In [9], [10], the transmitted symbols are scrambled in frequency-domain or time-domain. The interleaving of real and imaginary parts of symbols in [11] is based on the instantaneous channel state information between the legitimate transmitter and receiver, and the dummy data insertion and the resequenced training symbol can be found in [6].

Recently, as an alternative to OFDM, OFDM with offset quadrature amplitude modulation (OFDM/OQAM) has attracted a lot of attention because of its higher spectrum efficiency [12]. Different from OFDM, the orthogonality among sub-carriers in OFDM/OQAM systems holds only in the real field. Therefore, pure imaginary inter-carrier and inter-symbol interferences remain in the received symbol, which is known as intrinsic interference [13], [14]. This distinctive signal property requires the modification of the conventional signal processing methods designed for OFDM. To the best of our knowledge, until now only one PLE scheme has been proposed for OFDM/OQAM system [15], where the prototype filter (PF) is hopped over the time and frequency grid. However, the PF hopping not only is costly in implementation, but also brings real field non-orthogonality to the legitimate user.

In this paper, we propose a PLE method for OFDM/OQAM based on the intrinsic interference. In OFDM/OQAM systems, the imaginary part of transmitted symbols is usually unloaded to avoid its real-valued intrinsic interference. This consideration inspires us that the imaginary part of transmitted symbols can be used as an encryption key to obfuscate data symbols. Since the intrinsic interferences are widely spread and overlapped on the time-frequency grid, it is very difficult for the eavesdropper to completely remove the interference without the knowledge of the key and the loading pattern. Meanwhile, the legitimate receivers can eliminate the interference perfectly by calculating it in advance. We propose a key generation method and four key loading patterns. Then, the impact of channel estimation error and the robustness against ciphertext attacks are studied. Furthermore, the information leakage (IL) at the eavesdropper is analyzed, and numerical simulations are performed to demonstrate the validity of the proposed method.

II. PLE in OFDM/OQAM

A. System Model

In this paper, we consider an OFDM/OQAM system with N sub-carriers. Let $a_{m,n}$ be the transmitted pulse amplitude modulation (PAM) symbol, where m and n represent the time and the frequency indices, respectively. The baseband transmitted signal is given by

$$s(t) = \sum_{m=-\infty}^{\infty} \sum_{n=0}^{N-1} a_{m,n} \underbrace{e^{j\theta_{m,n}} p\left(t - m\frac{T}{2}\right) e^{j2\pi n f_0 (t - mT/2)}}_{p_{m,n}(t)}, \quad (1)$$

where $f_0 = 1/T$ is the sub-carrier spacing, $\theta_{m,n} = (m+n)\pi/2$ denotes the phase rotation of OQAM, and $p(t)$ represents the impulse response of the PF. After passing through the channel, the received signal is given by $y(t) = s(t) * h(t) + w(t)$, where $h(t)$ is the channel impulse response, and $w(t)$ is the additive white Gaussian noise (AWGN). If the channel

Manuscript received November 15, 2016; accepted January 2, 2017.
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

The authors are with the Department of Electrical and Information Systems, Graduate School of Engineering, Osaka Prefecture University, Sakai, Osaka 599–8531, Japan (e-mail: ss106025@edu.osakafu-u.ac.jp, lin@eis.osakafu-u.ac.jp, yamashita@eis.osakafu-u.ac.jp).

Digital Object Identifier XX.XXXX/LCOMM.XXXX.XXXXXXX

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/LCOMM.2017.2654442, IEEE Communications Letters

frequency response is nearly flat among neighboring subcarriers, the (m,n)th received symbol can be obtained as

$$R_{m,n} = \int_{-\infty}^{\infty} y(t)p^*_{m,n}(t)dt = H_{m,n}(a_{m,n} + jb_{m,n}) + N_{m,n}, \quad (2)$$

where $H_{m,n}$ is the nth frequency response of $h(t)$ at the mth symbol, and $N_{m,n}$ is the noise term [14]. The pure imaginary term $jb_{m,n}$ is the intrinsic interference consisting of the inter-carrier and the inter-symbol interferences from the neighboring time and frequency grids [13], [14]. After per subcarrier equalization, the transmitted symbol can be retrieved as $\hat{a}_{m,n} = \mathrm{Re}[R_{m,n}/H_{m,n}]$.

B. Intrinsic Interference Based PLE

Obviously, the complex-valued symbol cannot be transmitted in OFDM/OQAM since its intrinsic interference is not pure imaginary. Conversely, the real-valued interference caused by the imaginary part of the transmitted symbols can be used to conceal the data symbols.

Suppose the complex-valued transmitted symbol is $\dot{a}_{m,n} = a_{m,n} + ja'_{m,n}$, where $ja'_{m,n}$ represents an intentionally inserted pure imaginary symbol. After the equalization, the reconstructed symbol is given by

$$\hat{a}_{m,n} = a_{m,n} + b'_{m,n} + \mathrm{Re}[N_{m,n}/H_{m,n}], \quad (3)$$

where $b'_{m,n}$ is the real-valued intrinsic interference introduced by $ja'_{k,l}$ with $(k,l) \neq (m,n)$. The interference $b'_{m,n}$ obviously disrupts the correct demodulation of the data symbols $a_{m,n}$. On the other hand, if $ja'_{m,n}$ is known at the receiver, we can calculate $b'_{m,n}$ using the knowledge of the PF [13], [14], and then subtract it from $\hat{a}_{m,n}$. This means that the additional interference $b'_{m,n}$ acts as an encryption to the data symbols, and $ja'_{m,n}$ can be regarded as the key of the encryption. Noteworthy, this method does not change or modify the data symbols $a_{m,n}$, hence, can be used together with other PLE schemes to enhance the secrecy.

C. Key Generation and Key Patterns

We propose to create the key based on a pseudo-random sequence, which is generated by the linear feedback shift register (LFSR) because of its easy implementation. Firstly, consecutive Q bits $\boldsymbol{Q}_{m,n} = \{q_{g+0}, q_{g+1}, \cdots, q_{g+Q-1}\}$ are selected out of K-bit LFSR outputs, where $g = (m-1)N + n$. Then, $\boldsymbol{Q}_{m,n}$ is mapped into the corresponding decimal $u_{m,n}$, as a result, $a'_{m,n}$ is given as

$$a'_{m,n} = A \sin\left[\frac{u_{m,n}}{2^Q} \times 2\pi + \phi\right], \quad (4)$$

where A denotes the maximum amplitude of $a_{m,n}$, and ϕ is an intentional offset to avoid generating the same keys. A similar method can be found in [8]. Note that the logistic mapping in [9] is also a possible key generation method.

In addition to the key generation, the loading pattern is also very important since $b'_{m,n}$ actually comes from its neighboring $ja'_{k,l}$ for $(k,l) \neq (m,n)$. Four feasible patterns with different key loading densities are shown in Fig. 1, where the density R is given by the ratio of the number of key symbols to the total number of transmitted symbols.

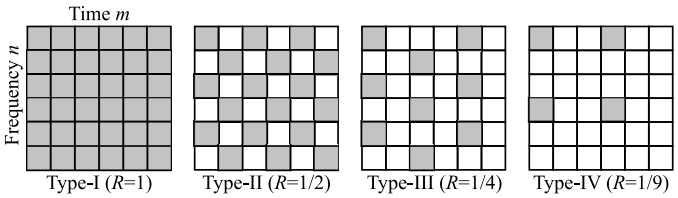

Fig. 1. Four loading patterns of key symbols. (The shadowed blocks indicate the intentionally loaded key symbols.)

III. Performance Analysis

In this section, the performance of the proposed PLE scheme is evaluated in terms of the impact of channel estimation error, the robustness against ciphertext attacks, and the IL at the eavesdropper, respectively.

A. Impact of Channel Estimation Error

While the perfect channel equalization is assumed in the previous sections, $H_{m,n}$ actually contains estimation error in practice. Let $\hat{H}_{m,n} = H_{m,n} + \Delta H_{m,n}$ denote the estimated channel frequency response, where $\Delta H_{m,n}$ represents the estimation error. After the equalization, subtracting $b'_{m,n}$ to decrypt the data symbols, we have

$$\hat{a}_{m,n} = \nu_I a_{m,n} + G_{m,n} + I_{m,n}, \quad (5)$$

where $\nu = 1/(1+\Delta H_{m,n}/H_{m,n})$, $G_{m,n} = (\nu_I - 1)b'_{m,n} - \nu_Q a'_{m,n}$, $I_{m,n} = -\nu_Q b_{m,n} + \mathrm{Re}[N_{m,n}/\hat{H}_{m,n}]$, and ν_I, ν_Q are real and imaginary part of ν, respectively. The second term $G_{m,n}$ is the residual interference caused by the encryption and the imperfect equalization, and its power $J_n = \mathbb{E}[|G_{m,n}|^2]$ can be used to measure the impact of the channel estimation error. Assuming ν_I, ν_Q and $a'_{m,n}$ are independent, we have

$$J_n = \mathbb{E}[|\nu_I - 1|^2]\mathbb{E}[|b'_{m,n}|^2] + \mathbb{E}[|\nu_Q|^2]\mathbb{E}[|a'_{m,n}|^2], \quad (6)$$

where $\mathbb{E}[a'_{m,n}b'_{m,n}] = 0$ since the each key is generated independently.

When $\mathbb{E}[|a'_{m,n}|^2]$ then $\mathbb{E}[|b'_{m,n}|^2]$ become large, more residual interference will be observed. On the other hand, increasing the power of $a'_{m,n}$ and $b'_{m,n}$ enhances the secrecy. Therefore, there is always a trade-off. The impact of the channel estimation error will be later examined in numerical simulation.

B. Robustness Against Ciphertext Attacks

Similar to the upper layer encryption schemes, the proposed method is also vulnerable to brute-force attacks on the ciphertext. The key space of $ja'_{m,n}$ is a good indicator to evaluate the robustness against the exhaustive key search. From (4), we can prepare 2^Q different keys. On the other hand, the possible values of $b'_{m,n}$ are clearly different from each loading pattern. The intrinsic interference $b'_{m,n}$ approximately consists of 20 neighboring keys $ja'_{k,l}$, where $k \in [m-3, m+3]$ and $l \in [n-1, n+1], \forall (k,l) \neq (m,n)$. Let $\Omega = \{\omega_1, \cdots, \omega_{20}\}$ denote an index set which represents the location of key symbols resulting in $b'_{m,n}$, where $\omega_i = 1, 0$ represents the state

TABLE I
LOCATION OF THE INDEX SET Ω

	$m-3$	$m-2$	$m-1$	m	$m+1$	$m+2$	$m+3$
$n-1$	ω_1	ω_2	ω_3	ω_4	ω_5	ω_6	ω_7
n	ω_8	ω_9	ω_{10}		ω_{11}	ω_{12}	ω_{13}
$n+1$	ω_{14}	ω_{15}	ω_{16}	ω_{17}	ω_{18}	ω_{19}	ω_{20}

whether the key is loaded or not. The time-frequency grid representation of Ω is given in Table I.

- Type-I: $b'_{m,n}$ is caused by 20 neighboring $ja'_{m,n}$, therefore, the index set is $\Omega^I = \{1, 1, \cdots, 1, 1\}$, and the number of $b'_{m,n}$ is given by $\mathcal{S}^I = 2^{20Q}$.
- Type-II: $b'_{m,n}$ is constructed by 10 neighboring $ja'_{m,n}$, however, there are two location patterns of $ja'_{m,n}$ depending on (m, n), that is, $\Omega_1^{II} = \{1, 0, 1, 0, \cdots, 0, 1, 0, 1\}$ and $\Omega_2^{II} = \{0, 1, 0, 1, \cdots, 1, 0, 1, 0\}$, respectively. Thus, the number of $b'_{m,n}$ is $\mathcal{S}^{II} = (2^{10Q} + 2^{10Q})/2 = 2^{10Q}$.
- Type-III and IV: Using similar calculation, we obtain $\mathcal{S}^{III} = (2^{4Q} + 2^{6Q})/2$ and $\mathcal{S}^{IV} = (7/9)2^{2Q} + (2/9)2^{3Q}$, respectively.

We note that $\mathcal{S}$ is actually the number of $b'_{m,n}$, not the number of "different" $b'_{m,n}$, which may be smaller than $\mathcal{S}$ since the different loading patterns have a potential to create the same intrinsic interference. The duplication of $b'_{m,n}$ can be avoided by the proper design of the key symbols $ja'_{m,n}$ and loading patterns. The detailed investigation of these issues is left as our future work.

The key space can be further expanded by increasing Q, while it is limited by the transmitter and receiver dynamic ranges. However, if $Q = 12$ bit, the key space becomes approximately 2.36×10^{21} in Type-III, which takes about 10^9 seconds for perfect encryption even the eavesdropper can perform 10^{12} decryption process per second.

C. IL at the Eavesdropper

It is known that the IL is very useful to evaluate the robustness of an encryption scheme [11]. In this paper, we assume M-PAM transmitted signal and AWGN channel for the sake of convenience. Suppose that each transmitted bit has equal probability of 0 or 1, the IL is given by $IL = \mathcal{G}(p_e)$, where p_e represents the bit error ratio (BER), and $\mathcal{G}(x) = 1 + (1-x)\log_2(1-x) + x\log_2 x$.

The (m, n)th received symbol at the eavesdropper is given by $\hat{a}_{m,n} = a_{m,n} + b'_{m,n} + N'_{m,n}$, where the noise term $N'_{m,n}$ is assumed to be a Gaussian random variable with zero mean and σ^2 variance. The BER with respect to the (m, n)th symbol is given by

$$p_e(m,n) = \sum_{\text{for all } b'_{m,n}} p(b'_{m,n}) p_e(\hat{a}_{m,n}|b'_{m,n}), \tag{7}$$

where $p(b'_{m,n}) = 1/\mathcal{S}$ and $p_e(\hat{a}_{m,n}|b'_{m,n})$ is the BER of M-PAM in the presence of the arbitrary offset $b'_{m,n}$. Let A_k denote the amplitude of kth constellation point, then the symbol pairwise error probability of confusing A_k with A_l when A_k is transmitted, is given by

$$P(A_k \to A_l) = \frac{1}{2}\text{erfc}\left(\frac{\alpha_l - A_k - b'_{m,n}}{\sqrt{2\sigma^2}}\right) - \frac{1}{2}\text{erfc}\left(\frac{\beta_l - A_k - b'_{m,n}}{\sqrt{2\sigma^2}}\right), \tag{8}$$

where (α_l, β_l) denote the decision area corresponding to the symbol A_l. Thus, the BER is then given by

$$p_e(\hat{a}_{m,n}|b'_{m,n}) = \frac{1}{M\log_2 M}\sum_{k=1}^{M}\sum_{l=1}^{M} d_{k,l} P(A_k \to A_l), \tag{9}$$

where $d_{k,l}$ represents the Hamming distance between the bits corresponding to A_k and A_l. The average IL is then given by

$$IL = \frac{1}{|\Lambda|}\sum_{(m,n)\in\Lambda} \mathcal{G}(p_e(m,n)), \tag{10}$$

where Λ denotes the set of all time and frequency index pairs in one OFDM/OQAM packet, and $|\Lambda|$ is the number of elements in Λ.

IV. NUMERICAL SIMULATIONS

The performance of the proposed method is evaluated through numerical simulations. In this simulation, the transmitted signal is an OFDM/OQAM signal with $N = 1024$ subcarriers having 15.0 kHz spacing, which is modulated by 4-PAM signaling, then, shaped by the PHYDYAS PF [16] with overlap factor 4. The keys are generated from $K = 24$ bit LFSR with $Q = 12$ bit, and $\phi = \sqrt{5}$. The channel is assumed to be time-invariant, and its power delay profile is based on the Extended Pedestrian A model.

Firstly, we evaluate the BERs of the legitimate user and the eavesdropper. From Fig. 2, we can see that the eavesdropper's BERs are floored because of the intentional interference caused by key symbols. On the other hand, the legitimate users can correctly retrieve the transmitted bits. However, compared to no encryption, around 4 dB SNR penalty can be observed for the Type-I loading pattern. It is not surprising that loading more key symbols enhances the secrecy, which requires more transmission power, as a consequence, the effective SNR of the original data symbol dropped. Nevertheless, the penalty is less than 1 dB in Type-IV, which is tolerable in practice.

The impact of the channel estimation error is also evaluated. Fig. 3 shows the BER with various channel estimation errors $\gamma = \mathbb{E}[|\Delta H_{m,n}|^2]/\mathbb{E}[|H_{m,n}|^2]$, where $\Delta H_{m,n}$ is assumed to be zero mean Gaussian random variable. In this simulation, Type-II key pattern is employed. For a large γ, the BER degradation induced by the encryption becomes severe. However, the SNR penalty is still less than 5 dB when $\gamma = 0.005$. On the other hand, the effect of key loading patterns is also investigated in the presence of channel estimation error. From Fig. 4, we can see that the denser key loading pattern results in more demodulation errors, which agrees with the result in Section III-A.

The IL in 4-PAM transmission is measured with respect to various noise variance. In this simulation, $p_e(m, n)$ is calculated by averaging the $p_e(\hat{a}_{m,n}|b'_{m,n})$ with randomly generated

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/LCOMM.2017.2654442, IEEE Communications Letters

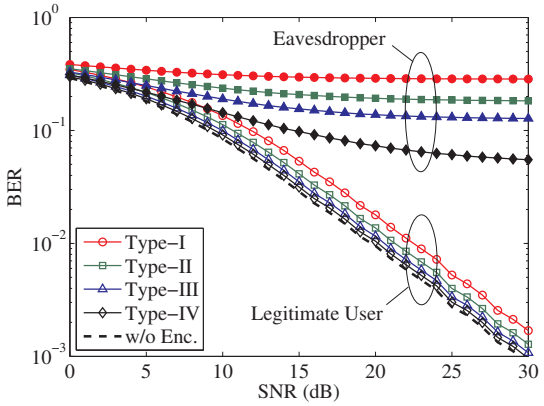

Fig. 2. BER in multipath Rayleigh fading channel.

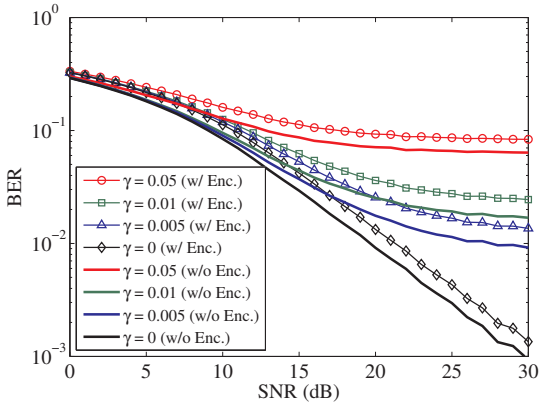

Fig. 3. BER with imperfect equalization, Type-II key loading pattern.

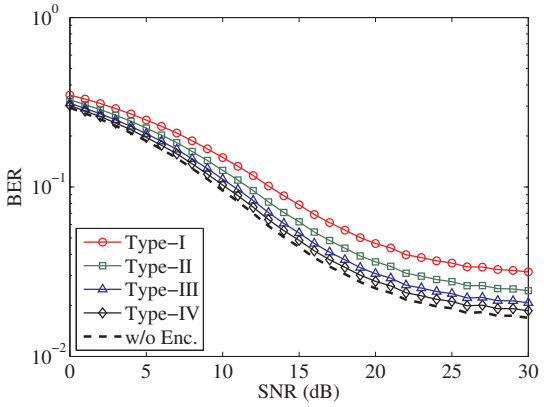

Fig. 4. BER with imperfect equalization, various key loading patterns, γ = 0.01.

keys. From Fig. 5, we can see that the ILs of the proposed method become very low compared to that without encryption. The Type-I pattern results at less than 0.2 bit IL over entire noise variance regime. Also, less than 0.4 bit IL can be achieved even when we use a sparser loading pattern, Type-II, which confirms the strong secrecy of the proposed method.

V. Conclusions

In this paper, a PLE was proposed for OFDM/OQAM systems. The proposed encryption employs additional imaginary

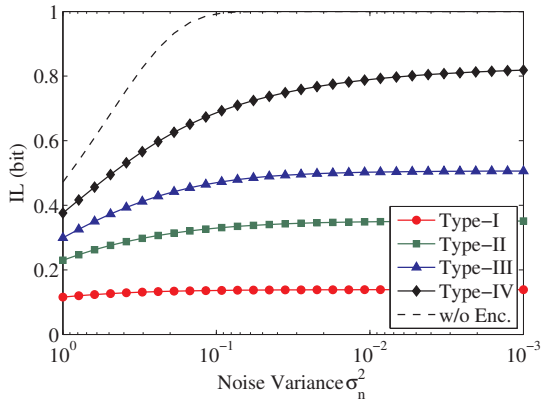

Fig. 5. IL versus noise variance σ_n^2.

symbols as keys so that their intrinsic interferences obfuscate the data symbols at eavesdroppers. The key generation and four loading patterns were proposed. The impact of channel estimation error, the robustness against ciphertext attacks, as well as the IL were investigated. The strong secrecy of the proposed encryption method was verified by numerical simulations.

References

[1] W. Trappe, "The challenges facing physical layer security," *IEEE Commun. Mag.*, vol. 53, no. 6, pp. 16–20, June 2015.
[2] S. Leung-Yan-Cheong and M. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. Inf. Theory*, vol. 24, no. 4, pp. 451–456, July 1978.
[3] F. Renna, N. Laurenti, and H. V. Poor, "Physical-layer secrecy for OFDM transmissions over fading channels," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 4, pp. 1354–1367, Aug. 2012.
[4] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180–2189, June 2008.
[5] C.-H. Lin, S.-H. Tsai, and Y.-P. Lin, "Secure transmission using MIMO precoding," *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 5, pp. 801–813, May 2014.
[6] J. Zhang, A. Marshall, R. Woods, *et al.*, "Design of an OFDM physical layer encryption scheme," *IEEE Trans. Veh. Technol.*, to be published.
[7] W. Zhang, C. Zhang, C. Chen, *et al.*, "Joint PAPR reduction and physical layer security enhancement in OFDMA-PON," *IEEE Photonics Technol. Lett.*, vol. 28, no. 9, pp. 998–1001, May 2016.
[8] R. Ma, L. Dai, Z. Wang, *et al.*, "Secure communication in TDS-OFDM system using constellation rotation and noise insertion," *IEEE Trans. Consum. Electron.*, vol. 56, no. 3, pp. 1328–1332, Aug. 2010.
[9] L. Zhang, X. Xin, B. Liu, *et al.*, "Secure OFDM-PON based on chaos scrambling," *IEEE Photonics Technol. Lett.*, vol. 23, no. 14, pp. 998–1000, July 2011.
[10] X. Yang, Z. Shen, X. Hu, *et al.*, "Chaotic encryption algorithm against chosen-plaintext attacks in optical OFDM transmission," *IEEE Photonics Technol. Lett.*, vol. 28, no. 22, pp. 2499–2502, Nov. 2016.
[11] H. Li, X. Wang, and Y. Zou, "Dynamic subcarrier coordinate interleaving for eavesdropping prevention in OFDM systems," *IEEE Commun. Lett.*, vol. 18, no. 6, pp. 1059–1062, June 2014.
[12] B. Farhang-Boroujeny, "OFDM versus filter bank multicarrier," *IEEE Signal Process. Mag.*, vol. 28, no. 3, pp. 92–112, May 2011.
[13] P. Siohan, C. Siclet, and N. Lacaille, "Analysis and design of OFDM/OQAM systems based on filterbank theory," *IEEE Trans. Signal Process.*, vol. 50, no. 5, pp. 1170–1183, May 2002.
[14] C. Lélé, J. -P. Javaudin, R. Legouable, *et al.*, "Channel estimation methods for preamble-based OFDM/OQAM modulations," *Wiley Eur. Trans. Telecommun.*, vol. 19, no. 7, pp. 741–750, 2008.
[15] V. Lücken, T. Singh, Ö Cepheli, *et al.*, "Filter hopping: Physical layer secrecy based on FBMC," in *Proc. IEEE WCNC*, Mar. 2015, pp. 568–573.
[16] M. Bellanger *et al.*, "FP7-ICT Project PHYDYAS-Physical Layer for Dynamic Spectrum Access and Cognitive Radiio," 2010. [Online]. Available: http://www.ict-phydyas.org.