Research Article Vol. 26, No. 26 | 24 Dec 2018 | OPTICS EXPRESS 34031

Optics EXPRESS

Secure and private NOMA VLC using OFDM with two-level chaotic encryption

YANBING YANG,[1] CHEN CHEN,[2,*] WEI ZHANG,[3] XIONG DENG,[4] PENGFEI DU,[2] HELIN YANG,[2] WEN-DE ZHONG,[2] AND LIANGYIN CHEN[1]

[1] *College of Computer Science, Sichuan University, Chengdu 610065, China*
[2] *School of Electrical and Electronic Engineering, Nanyang Technological University, 50 Nanyang Avenue, 639798, Singapore*
[3] *Institute of Cyberspace Security, China Electronic Technology Cyber Security Co. Ltd, Chengdu 610041, China*
[4] *Department of Electrical Engineering, Eindhoven University of Technology (TU/e), Flux Building, 5600MB Eindhoven, Netherlands*
[*] *chen0884@e.ntu.edu.sg*

Abstract: In this paper, we propose and demonstrate a secure and private non-orthogonal multiple access (NOMA) based visible light communication (VLC) system. Orthogonal frequency division multiplexing (OFDM) modulation is applied in the system and a two-level chaotic encryption scheme is further implemented, which can guarantee both the security of legitimate users against eavesdroppers and the privacy among all the legitimate users. An experimental demonstration with two legitimate users and one eavesdropper successfully verifies the feasibility of the proposed secure and private NOMA VLC system. To the best of our knowledge, it is the first time that simultaneous security and privacy improvement is considered for NOMA VLC systems.

1. Introduction

Visible light communication (VLC) utilizing illuminating white light-emitting diodes (LEDs) has attracted tremendous attention in recent years, where the LEDs in VLC systems serve a dual-function of simultaneous illumination and wireless communication [1]. Although VLC enjoys many inherent advantages such as huge license-free spectrum, low-cost front-ends and strong immunity to electromagnetic interference (EMI), the achievable capacity of VLC systems is greatly limited by the small 3-dB modulation bandwidth of off-the-shelf white LEDs [2]. In order to improve the capacity of white LEDs based VLC systems, several techniques have been proposed such as orthogonal frequency division multiplexing (OFDM) using high-order quadrature amplitude modulation (QAM) constellations, multiple-input-multiple-output (MIMO) transmission, and frequency-domain equalization [3–5].

As a promising candidate for the 5th generation (5G) wireless networks, power domain non-orthogonal multiple access (NOMA) has been widely investigated in literature [6]. Due to its high spectral efficiency, NOMA has also been applied for capacity improvement in multi-user VLC systems [7–9]. So far, efforts have been made to improve the performance of NOMA VLC systems, for example, the optimization of user grouping and power allocation [10], the combination of NOMA with orthogonal frequency division multiplexing access (OFDMA) [11], the mitigation of error propagation in NOMA [12, 13], the application of NOMA in MIMO-VLC systems [14], etc.

In typical indoor VLC systems, the optical signal can be well confined within the room since line-of-sight (LOS) transmission is usually adopted [2]. However, due to the inherent broadcast nature of VLC, the confidential information transmitted over VLC channels might be

#346179 https://doi.org/10.1364/OE.26.034031
Journal © 2018 Received 17 Sep 2018; revised 14 Nov 2018; accepted 6 Dec 2018; published 14 Dec 2018

eavesdropped by unintended or unauthorized users [15,16]. To date, several physical-layer security enhancement techniques have been reported in literature for VLC. In [17], a light encryption scheme using devices having LED and camera image sensor was proposed for VLC systems, where the light encrypter acts as an encryption gateway for signals in optical domain. In [18], a secure VLC system using light-panel and mobile-phone image sensor was demonstrated, where the security was achieved by employing a specially developed mobile-phone application program (APP). Specifically, chaotic encryption based physical-layer security enhancement techniques have also been applied in VLC systems [19,20]. In addition to VLC, the near-infrared wavelength band has also been widely studied to provide indoor wireless access to end users [21,22]. Due to the use of a semiconductor laser as the transmitter, analog optical chaos can be adopted to provide security in conventional near-infrared optical wireless communication systems [23]. However, since non-coherent LEDs are generally used as optical transmitters, the analog optical chaos scheme is not applicable in typical VLC systems.

Although secure VLC systems have been investigated in recent years, the physical-layer security issue in NOMA enabled VLC systems has not yet been considered. Furthermore, since power domain superposition and successive interference cancellation (SIC) are generally adopted in NOMA VLC systems, one legitimate user can decode the signal intended for another legitimate user, resulting in a privacy issue among all legitimate users served by the NOMA VLC system. To the best of our knowledge, no work has ever been done on the improvement of both security and privacy of NOMA VLC systems.

In this paper, we for the first time propose and experimentally demonstrate a secure and private NOMA VLC system. By using OFDM modulation with two-level chaotic encryption, the security of legitimate users against the eavesdroppers can be guaranteed and the privacy among all the legitimate users can also be ensured without affecting the bit error rate (BER) performance of the legitimate users. The feasibility of the proposed secure and private NOMA VLC system is successfully verified by proof-of-concept experiments with two legitimate users and one eavesdropper.

2. Secure and private NOMA VLC system

2.1. System model

We first introduce the model of an indoor NOMA VLC system with multiple users. For simplicity and without loss of generality, we assume that there are two legitimate users (user 1 and user 2) and one eavesdropper in the NOMA VLC system. Figure 1 illustrates the system model, where user 1 is assumed to be closer to the LED than user 2 and thus user 2 is allocated with more electrical power than user 1, so as to successfully perform SIC. As can be seen from Fig. 1, the NOMA VLC system is vulnerable to eavesdropping when an eavesdropper is located within the illuminated area of the LED, due to the LOS characteristic and the broadcasting nature of VLC, which leads to a security problem in the NOMA VLC system. Moreover, the privacy among all the legitimate users also cannot be guaranteed due to the use of SIC. Hence, security and privacy are two important issues that both need to be addressed in practical NOMA VLC systems.

Let $s_1(t)$ and $s_2(t)$ represent the signals intended for user 1 and user 2, respectively. The transmitted signal $x(t)$ of the LED can be expressed by

$$x(t) = \sqrt{p_1}s_1(t) + \sqrt{p_2}s_2(t) + I_{\text{DC}}, \tag{1}$$

where p_1 and p_2 are the electrical powers allocated to user 1 and user 2, respectively, and I_{DC} is the DC bias of the LED. The total electrical power is given by $p_{tot} = p_1 + p_2$ and the power allocation ratio between user 1 and user 2 is defined by $\alpha = p_1/p_2$. After free-space propagation, the received electrical signals at user 1, user 2 and the eavesdropper are respectively given by

$$y_1(t) = Rh_1(t)x(t) + z_1(t), \tag{2}$$

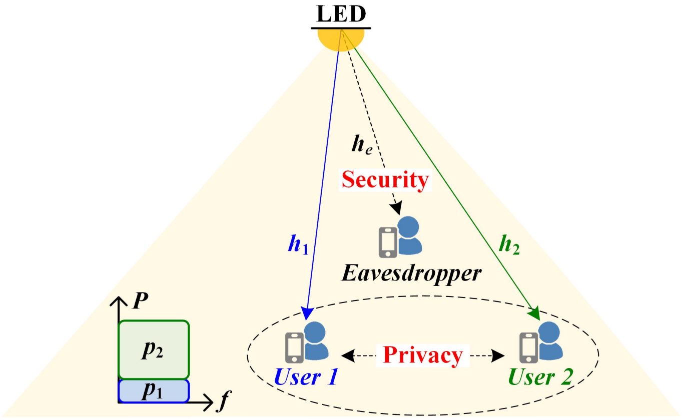

Fig. 1. Illustration of a NOMA VLC system with two legitimate users and one eavesdropper.

$$y_2(t) = Rh_2(t)x(t) + z_2(t), \tag{3}$$

$$y_e(t) = Rh_e(t)x(t) + z_e(t), \tag{4}$$

where R is the responsivity of the photodetectors (PDs), h_1, h_2 and h_e are the corresponding optical channel gains, and $z_1(t)$, $z_2(t)$ and $z_e(t)$ are the corresponding additive noises.

2.2. NOMA-OFDM with two-level chaotic encryption

Figure 2 depicts the principle of the proposed NOMA-OFDM scheme with two-level chaotic encryption in a two-user case, where M_1-QAM and M_2-QAM constellations are adopted for user 1 and user 2, respectively. For simplicity of notation, we denote it as (M_1, M_2)-QAM in the following descriptions.

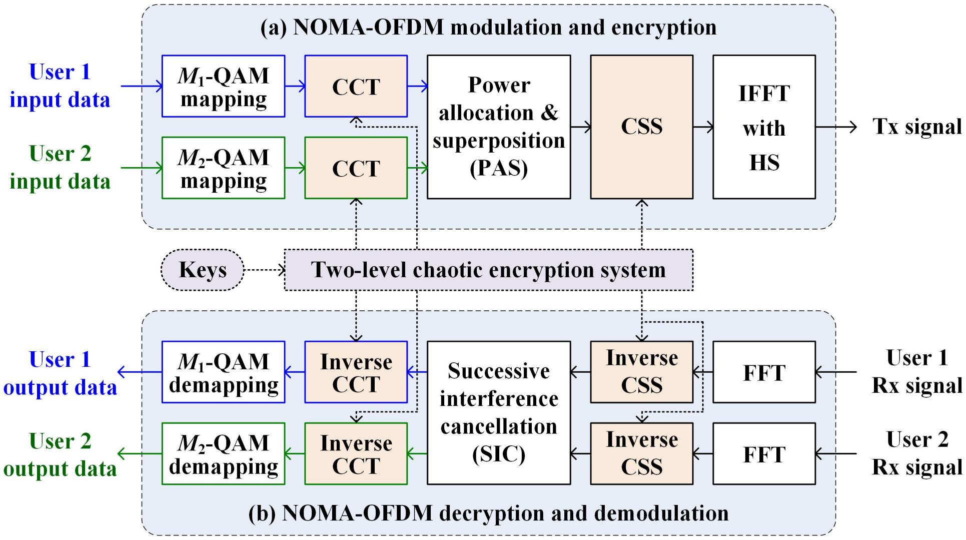

Fig. 2. Principle of (M_1, M_2)-QAM based two-user NOMA-OFDM with two-level chaotic encryption: (a) modulation and encryption and (b) decryption and demodulation.

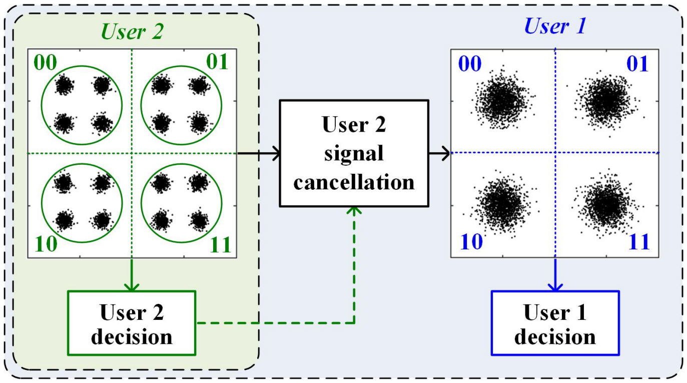

Fig. 3. Illustration of SIC-aided decoding for (4, 4)-QAM based NOMA-OFDM signal.

In the NOMA-OFDM modulation and encryption, as shown in Fig. 2(a), the input data of two legitimate users are first mapped to (M_1, M_2)-QAM symbols, and then the QAM symbols of each user are encrypted through the first-level chaotic encryption, i.e. chaotic constellation transformation (CCT), which scrambles the bit-to-symbol mapping for each user. Subsequently, power allocation and superposition (PAS) is executed and parallel superposed QAM symbols corresponding to the data-carrying subcarriers for the inverse fast Fourier transform (IFFT) are obtained. After that, the second-level chaotic encryption, i.e. chaotic subcarrier scrambling (CSS), is further performed, which scrambles the symbol-to-subcarrier mapping for both users. Finally, the transmitted electrical signal is generated by performing IFFT with Hermitian symmetry (HS). In the NOMA-OFDM decryption and demodulation, as can be seen from Fig. 2(b), the received signal of each user is first transformed back to the frequency domain via fast Fourier transform (FFT), and then the first-level chaotic decryption, i.e. inverse CSS, is conducted. After performing SIC, the second-level chaotic decryption, i.e. inverse CCT, is further executed for each user. The output data of each user can be obtained through QAM demapping. Figure 3 illustrates the principle of SIC-aided decoding for the (4, 4)-QAM based NOMA-OFDM signal. Since user 2 is allocated with more power than user 1, user 2 can directly decode the received (4, 4)-QAM constellation without performing interference cancellation by treating the 4-QAM signal of user 1 as noise. In contrast, user 1 first decodes the signal for user 2 and then subtracts it from the received signal. Hence, user 1 can decode the signal without interference from user 2 under perfect SIC. It can be seen that only inverse CCT is performed after SIC at the receiver. Since only the bit-to-symbol mapping is scrambled after CCT and the inverse CCT process can always be successfully performed as long as users have the correct keys, it is believed that error propagation of SIC decoding only affects the demodulation of QAM symbols, which has no effect on the decryption (i.e., inverse CCT) process. For simplicity and without loss of generality, we consider perfect SIC in this work, considering that the error propagation effect can be efficiently eliminated by using symmetric superposition coding [12] or constellation partitioning coding [13].

The detailed procedures of the two-level chaotic encryption, i.e. CCT and CSS, are introduced in the following. Without loss of generality, we assume that there are K users in the NOMA VLC system and totally N OFDM symbols to be transmitted for each user, with each OFDM symbol consisting of F data-carrying subcarriers. Let $I_{n,f,k}$ and $Q_{n,f,k}$ represent the in-phase (I) and quadrature-phase (Q) parts of the unencrypted M-QAM symbol in the n-th ($n = 1, 2, \cdots, N$) OFDM symbol at the f-th ($f = 1, 2, \cdots, F$) data subcarrier of the k-th ($k = 1, 2, \cdots, K$) user, respectively. After performing the first-level chaotic encryption, i.e. CCT, the corresponding I and Q parts of the encrypted M-QAM symbol can be expressed by

$$\begin{bmatrix} I'_{n,f,k} \\ Q'_{n,f,k} \end{bmatrix} = \begin{bmatrix} 1 & a_{n,f,k} \\ b_{n,f,k} & a_{n,f,k}b_{n,f,k}+1 \end{bmatrix} \begin{bmatrix} \frac{I_{n,f,k}+m-1}{2} \\ \frac{Q_{n,f,k}+m-1}{2} \end{bmatrix} \mathrm{mod}(m) - m + 1, \tag{5}$$

where $a_{n,f,k}$ and $b_{n,f,k}$ ($a_{n,f,k}, b_{n,f,k} \in \{1, 2, \cdots, m\}$) are two integer parameters and $m = \log_2 M$.

It can be seen from Fig. 2 that the first-level chaotic encryption CCT is performed for each user, while the second-level chaotic encryption CSS is executed for all the users after power domain superposition. Assuming the input QAM symbol vector corresponding to the F data subcarriers in the n-th OFDM symbol is given by $\mathbf{s}_n = \{s_{n,1}, s_{n,2}, \cdots, s_{n,F}\}^T$ where $(\cdot)^T$ denotes the transpose operation, the output QAM symbol vector $\mathbf{w}_n = \{w_{n,1}, w_{n,2}, \cdots, w_{n,F}\}^T$ after performing CSS can be represented by

$$\mathbf{w}_n = src\{\mathbf{s}_n, \mathbf{p}_n\}, \tag{6}$$

where $src\{\cdot,\cdot\}$ denotes the scrambling function and $\mathbf{p}_n = \{p_{n,1}, p_{n,2}, \cdots, p_{n,F}\}^T$ is the permutation vector. The scrambling function scrambles $\mathbf{s}_n$ according to $\mathbf{p}_n$ which indicates the new positions of the subcarriers in the n-th OFDM symbol.

In order to successfully perform CCT and CSS, the integer parameters $a_{n,f,k}$, $b_{n,f,k}$ and the permutation vector $\mathbf{p}_n$ should be determined first. In this work, 2D Logistic map and piecewise linear Chaotic map (PWLCM) are adopted [24, 25], which are respectively defined by Eqs. (7) and (8):

$$\begin{cases} x_{t+1} = \alpha_1 x_t(1-x_t) + \beta_1 y_t^2 \\ y_{t+1} = \alpha_2 y_t(1-y_t) + \beta_2(x_t^2 + x_t y_t) \end{cases}, \tag{7}$$

$$z_{t+1} = F_\gamma(z_t) = \begin{cases} z_t/\gamma, & 0 < z_t < \gamma \\ (z_t-\gamma)/(0.5-\gamma), & \gamma \le z_t < 0.5 \\ F_\gamma(1-z_t), & 0.5 \le z_t < 1 \end{cases}, \tag{8}$$

where $0 < x_t \le 1, 0 < y_t \le 1, 0 < z_t < 1$, and t is the discrete time index. When $2.75 < \alpha_1 \le 3.4$, $2.75 < \alpha_2 \le 3.45$, $0.15 < \beta_1 \le 0.21$, $0.13 < \beta_2 \le 0.15$, and $0 < \gamma < 0.5$, the systems defined by Eqs. (7) and (8) fall into the chaotic domain. It has been verified in [24, 25] that the sequences x_t, y_t and z_t generated by such systems have high unpredictability, randomness and sensitivity to the initial values.

By utilizing the systems given by Eqs. (7) and (8), the integer parameters $a_{n,f,k}$, $b_{n,f,k}$ and the permutation vector $\mathbf{p}_n$ can be successfully obtained. For the k-th user, $a_{n,f,k}$ and $b_{n,f,k}$ are generated by the states x_t^k and y_t^k, which can be expressed by

$$a_{n,f,k} = mod\left(ceil\left(x^k_{(n-1)F+f} \cdot 10^{15}\right), m\right) + 1, \tag{9}$$

$$b_{n,f,k} = mod\left(ceil\left(y^k_{(n-1)F+f} \cdot 10^{15}\right), m\right) + 1, \tag{10}$$

where $ceil(\cdot)$ denotes the upper round operation and $mod(\cdot, m)$ returns the remainder of an input divided by m. Moreover, $\mathbf{p}_n$ is generated by the state z_t, which can be obtained by

$$\mathbf{p}_n = sort\{[z_{(n-1)F+1}, z_{(n-1)F+2}, \cdots, z_{nF}]^T\}, \tag{11}$$

where $sort\{\cdot\}$ is the sorting function which returns the index vector of the elements of the input vector by sorting these elements in a descending order.

Based on Eqs. (9)-(11), we can obtain the integer parameters $a_{n,f,k}$, $b_{n,f,k}$ and the permutation vector $\mathbf{p}_n$, and hence the two-level chaotic encryption can be successfully implemented. Evidently, the corresponding decryption of the two-level chaotic encryption can be achieved by using the inverse processes of CSS and CCT, which is omitted here for brevity. Since CSS is executed after power domain superposition, the permutation vector $\mathbf{p}_n$ is shared by all the users. However, CCT is performed for each user and hence different users should have different integer parameters. Hence, the initial value z_0 and the parameter γ in Eq. (8) can be set as the shared security keys for all users to perform CSS, while the initial values x_0^k, y_0^k and the parameters α_1^k, α_2^k, β_2^k, β_2^k in Eq. (7) can be set as the private security keys for the k-th user to perform CCT. The security keys are assumed to be pre-shared between the LED transmitter and the legitimate users, and a pilot-aided security key agreement approach can be employed [26].

Although only two legitimate users are considered in the prototypical NOMA VLC system, the proposed two-level chaotic encryption scheme is applicable to the system with more than two legitimate users. Moreover, since the two-level chaotic encryption is performed for each individual user in the frequency domain, it is also feasible to extend the proposed scheme to practical systems with multiple LEDs, for example, MIMO-NOMA based VLC systems or multi-cell NOMA VLC systems. The main limitation for the NOMA VLC system to support more users is the design of low-complexity but efficient user pairing/grouping and power allocation strategies, which is beyond the scope of this paper.

3. Experimental setup

Figure 4 depicts the experimental setup of a secure and private NOMA VLC system with two legitimate users and one eavesdropper, employing (4, 4)-QAM NOMA-OFDM modulation with two-level chaotic encryption. The transmitted (4, 4)-QAM based NOMA-OFDM signal with a power allocation ratio α is generated offline by MATLAB and uploaded to an arbitrary waveform generator (AWG, Spectrum M4x.6622-x4) with a gain of 500 and a sampling rate of 50 MSa/s. Subsequently, the obtained signal is amplified by an electrical amplifier (Amp) and a 3.5-V DC bias is added via a bias-tee (bias-T). The resultant signal is then used to drive a white LED (Luxeon SR-12 Rebel Star/O). After 100-cm free-space propagation, the light is detected by two legitimate users (user 1 and user 2) and one eavesdropper (eav). In this setup, user 1 is assumed to face towards the LED while user 2 has an position offset of 15 cm from user 1. Moreover, the eavesdropper is located at the middle position between user 1 and user 2. Each user and the eavesdropper are individually equipped with an optical lens, a blue filter (BF) and a PD (Thorlabs PDA10A). The detected signals are sampled by a mixed domain oscilloscope (Tektronix MDO3104) with a sampling rate of 500 MSa/s, which are further processed offline. The insets (a) and (b) in Fig. 4 illustrate the waveform and the constellation diagram of the transmitted (4, 4)-QAM based NOMA-OFDM signal, respectively.

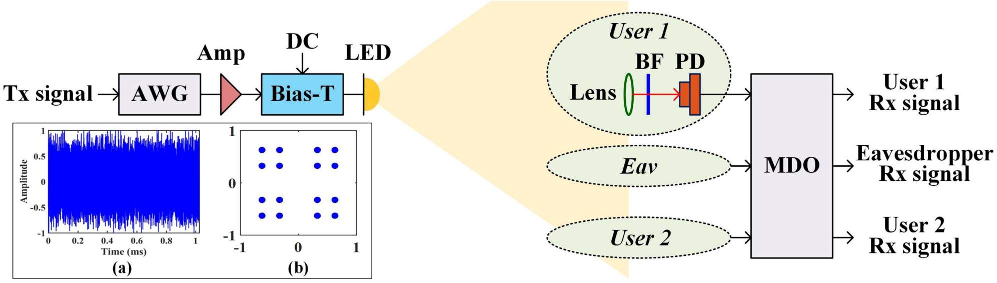

Fig. 4. Experimental setup of a secure and private NOMA VLC system with two legitimate users and one eavesdropper using (4, 4)-QAM OFDM with two-level chaotic encryption.

The digital (4, 4)-QAM based NOMA-OFDM signal is generated offline by MATLAB with an

IFFT size of 256. A total of 77 (2nd to 78th) subcarriers are used to modulate valid data and thus the bandwidth of the NOMA-OFDM signal is calculated by $(50 \times 77) / 256 \approx 15$ MHz. No cyclic prefix (CP) is used and 1600 OFDM symbols are transmitted for BER measurement. Therefore, the data rate of each legitimate user is given by $\log_2 4 \times 15 = 30$ Mbit/s and the sum rate of two legitimate users is 60 Mbit/s.

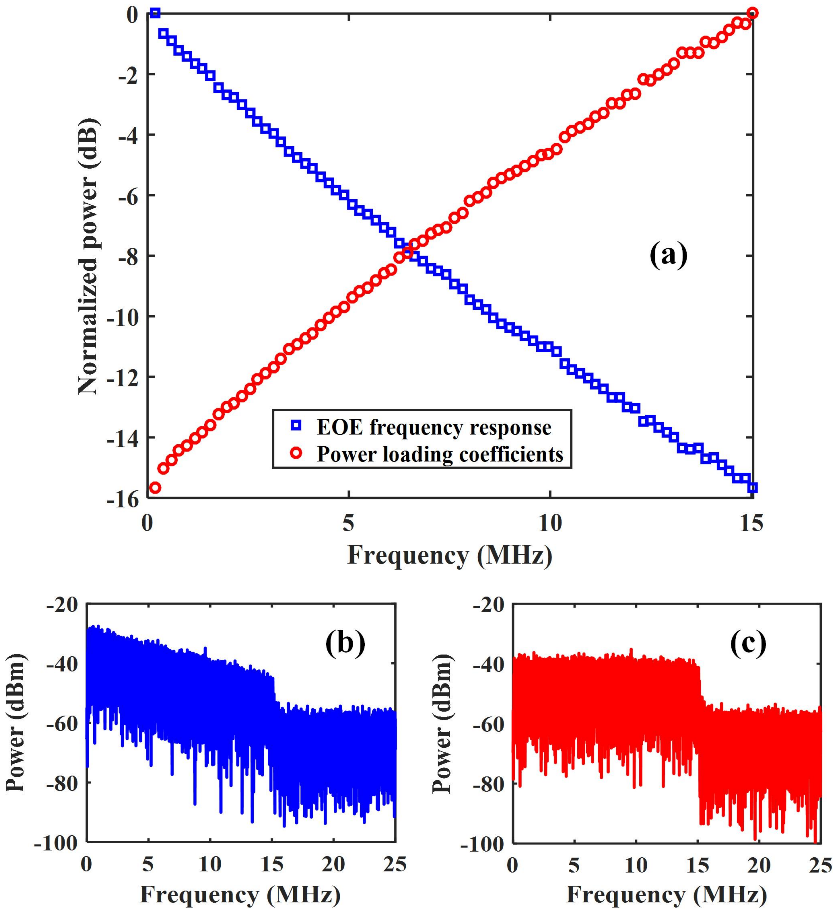

Fig. 5. (a) Measured frequency response and the corresponding power loading coefficients for digital pre-FDE and the received electrical spectra (b) before and (c) after digital pre-FDE.

It is measured that the 3-dB modulation bandwidth of the VLC system is only 2.4 MHz. In order to extend the 3-dB modulation bandwidth, digital pre-frequency domain equalization (pre-FDE) is performed [27]. Figure 5(a) illustrates the measured electrical-optical-electrical (EOE) frequency response of the system and the corresponding power loading coefficients for digital pre-FDE. The received electrical spectra before and after pre-FDE are shown in Figs. 5(b) and 5(c), respectively. As we can see, a power attenuation of 15.7 dB is observed over the 15-MHz OFDM band. However, the received electrical spectrum is greatly flattened after performing digital pre-FDE, which has a power attenuation less than 3 dB.

4. Results and discussions

4.1. Security and privacy analysis

We first evaluate the security and privacy performance of the proposed NOMA VLC system enabled by the two-level chaotic encryption scheme. For a digital chaotic encryption scheme, key space is usually adopted to evaluate the encryption performance of the scheme. In the proposed system, the security of legitimate users against eavesdroppers is achieved by both the first-level CCT and the second-level CSS, while the privacy among all the legitimate users can be guaranteed by the first-level CCT. In principle, only using the first-level CCT for each user can also provide both security and privacy for the NOMA VLC system. However, the key space using only the first-level CCT might be relatively small. In order to substantially enlarge the key space and hence improve the security of legitimate users against eavesdroppers, the second-level CSS is further considered. In the following, the key space with respect to the security of legitimate users against eavesdroppers and the privacy among all the legitimate users are analyzed.

For the first-level CCT, as discussed in Section 2.2, totally six parameters, i.e., x_0^k, y_0^k, α_1^k, α_2^k, β_2^k and β_2^k, can be set as the private security keys for the k-th user. According to the IEEE standard for binary floating-point arithmetic [28], the computational precision of a 64-bit double-precision number is approximately 10^{-15}. Since $0 < x_0^k \leq 1$, $0 < y_0^k \leq 1$, $2.75 < \alpha_1^k \leq 3.4$, $2.75 < \alpha_2^k \leq 3.45$, $0.15 < \beta_1^k \leq 0.21$, and $0.13 < \beta_2^k \leq 0.15$, the key space of the first-level CCT can be calculated by $10^{15}\times10^{15}\times0.65\times10^{15}\times0.7\times10^{15}\times0.06\times10^{15}\times0.02\times10^{15} = 5.46\times10^{86}$. Similarly, for the second-level CSS, z_0 and γ can be set as the shared security keys for all users. Since $0 < z_0 < 1$ and $0 < \gamma < 0.5$, the key space of the second-level CSS can be obtained by $10^{15} \times 0.5 \times 10^{15} = 5 \times 10^{29}$.

Based on the above analysis, the key space with respect to the security of legitimate users against eavesdroppers is contributed by both the first-level CCT and the second-level CSS which is given by $5.46 \times 10^{86} \times 5 \times 10^{29} = 2.73 \times 10^{116}$. Moreover, the key space with respect to the privacy among all the legitimate users is only contributed by the first-level CCT which is given by 5.46×10^{86}. As we can see, the key space with respect to the security of legitimate users against eavesdroppers is substantially enlarged from 5.46×10^{86} to 2.73×10^{116} when adopting the two-level chaotic encryption scheme in comparison to that using only the first-level CCT.

4.2. PAPR analysis

In the next, we also compare the peak-to-average power ratio (PAPR) of the time-domain NOMA signal with and without encryption. As shown in Fig. 6, the time-domain NOMA signal has the same PAPR performance for three different cases: (1) without encryption; (2) with only CCT; (3) with both CCT and CSS. This is because the adopted two-level chaotic encryption only scrambles the bit-to-symbol mapping and the symbol-to-subcarrier mapping, which has no effect on the PAPR performance of the time-domain NOMA signal.

4.3. Measured BER performance

After that, we measure the BER versus power allocation ratio of the (4, 4)-QAM based NOMA-OFDM signal for the two legitimate users with perfect SIC in the secure and private NOMA VLC system. As shown in Fig. 7, nearly the same BER performance can be achieved with and without the two-level chaotic encryption for each legitimate user. Moreover, the BER of user 1 is gradually reduced with the increase of the power allocation ratio and the BER reaches the forward error correction (FEC) threshold of 3.8×10^{-3} when the power allocation ratio is 0.16. In contrast, the BER of user 2 is gradually increased with the increase of the power allocation ratio and the maximum power allocation ratio to reach the FEC threshold is 0.31. It also can be seen that the lowest average BER with and without encryption is achieved at the power allocation ratio of 0.25. The insets in Fig. 7 illustrates the corresponding (4, 4)-QAM constellation diagrams.

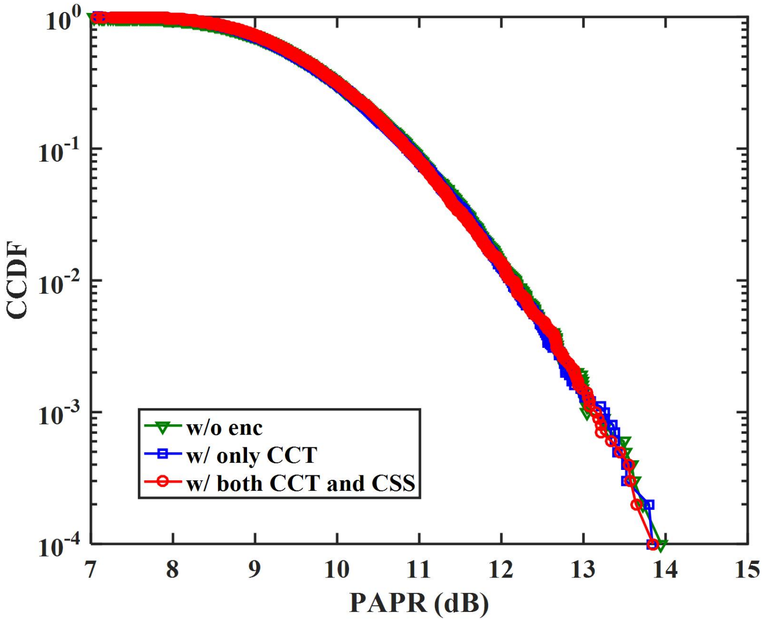

Fig. 6. Comparison of PAPR performance of the time-domain NOMA signal with and without encryption. w/o: without; w/: with; enc: encryption.

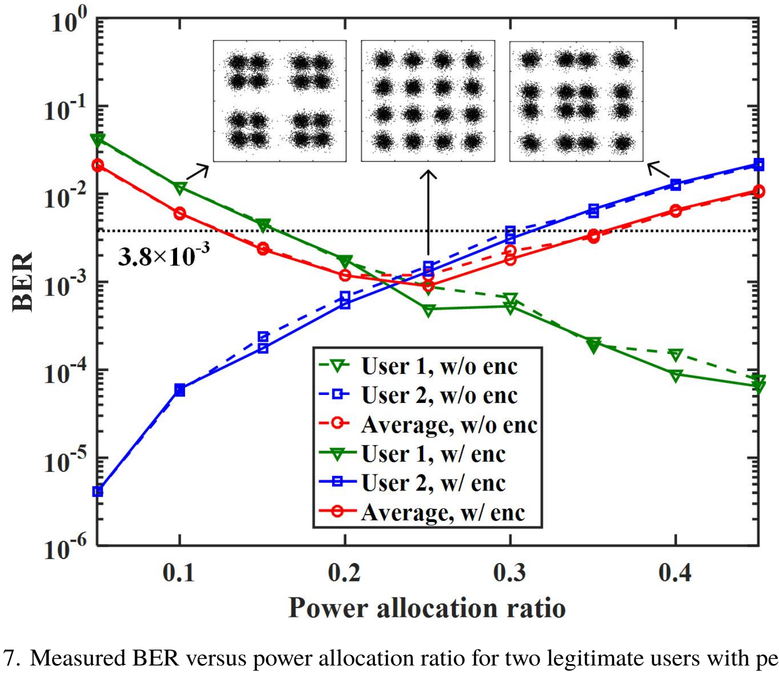

Fig. 7. Measured BER versus power allocation ratio for two legitimate users with perfect SIC. w/o: without; w/: with; enc: encryption.

Then, we evaluate the BER performance of the eavesdropper and three different scenarios are considered: (1) the eavesdropper has no key at all; (2) the eavesdropper only has the key for CCT; (3) the eavesdropper only has the key for CSS. As can be seen from Fig. 8(a), the BER of the eavesdropper decoding the signal of a legitimate user, either user 1 or user 2, is always about 0.5

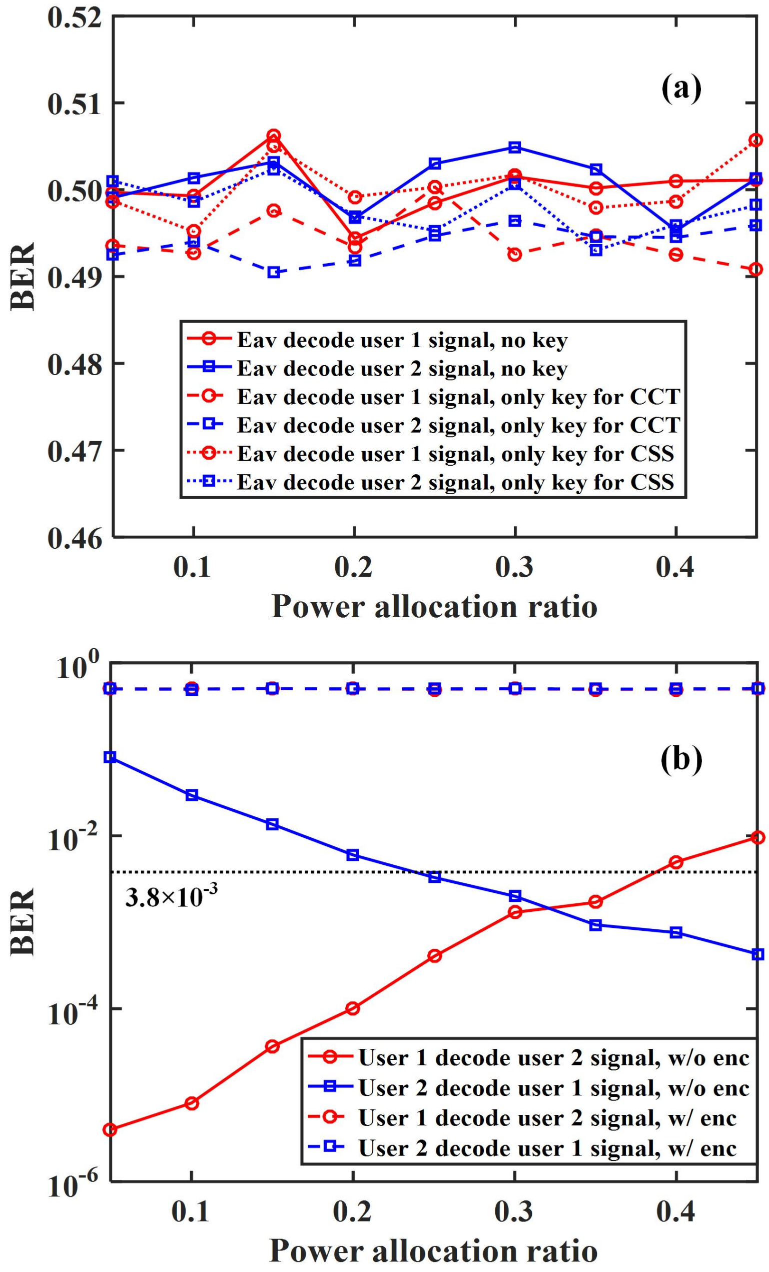

Fig. 8. Measured BER versus power allocation ratio for (a) eavesdropper decoding legitimate users' signal and (b) one legitimate user decoding the signal of another legitimate user. eav: eavesdropper; w/o: without; w/: with; enc: encryption.

under all three scenarios, due to the incorrect bit-to-symbol mapping and/or symbol-to-subcarrier mapping. It indicates that the eavesdropper cannot get any useful information from the legitimate users for an arbitrary power allocation ratio, unless the eavesdropper have keys for both CCT and CSS at the same time. Furthermore, the privacy between two legitimate users is evaluated. As shown in Fig. 8(b), user 1 can decode the signal of user 2 successfully when the power allocation ratio is equal or less than 0.39 if the NOMA VLC system is not encrypted. Similarly, without encryption, user 1's signal can be decoded successfully by user 2 when the power allocation ratio is equal or larger than 0.24. Hence, the privacy between legitimate users cannot be efficiently guaranteed if the NOMA VLC system is not encrypted. However, when the proposed NOMA-OFDM scheme with two-level chaotic encryption is implemented in the NOMA VLC system, as can be observed from Fig. 8(b), the BER of a legitimate user decoding the signal of another legitimate user is always about 0.5 for an arbitrary power allocation ratio, suggesting significantly enhanced privacy between two legitimate users.

5. Conclusion

In this paper, we have proposed and experimentally demonstrated a novel secure and private NOMA VLC system by employing OFDM modulation with two-level chaotic encryption. In comparison to the conventional NOMA VLC system without encryption, both the security of legitimate users against the eavesdroppers and the privacy among all the legitimate users can be guaranteed in the proposed encrypted NOMA VLC system. The experimental results show that nearly the same BER performance can be achieved for each legitimate user with and without the two-level chaotic encryption. Moreover, the eavesdropper cannot get any useful information from the legitimate users due to the lack of keys for successful decryption. It has also be verified that a legitimate user cannot decode the signal intended for another legitimate user during the process of SIC. Therefore, the proposed NOMA VLC system is promising for future high-speed secure and private indoor wireless communications.

Funding

National Natural Science Foundation of China (NSFC) (61373091); Fundamental Research Funds for the Central Universities (20822041B4232); NSFC and Civil Aviation Administration of China (CAAC) (U1533203); The Key Technology R&D Program of Sichuan Province (2016GZ0068, Science and Technology Department of Sichuan Province, China); The Collaborative Innovation of Industrial Cluster Project of Chengdu (2016-XT00-00015-GX); Civil Aviation Airport United Laboratory of Second Research Institute, CAAC and Sichuan University of Chengdu (2015-YF04-00050-JH).

References

1. T. Komine and M. Nakagawa, "Fundamental analysis for visible-light communication system using LED lights," IEEE Trans. Consum. Electron. **50**(1), 100–107 (2004).
2. H. Haas, "Visible light communication," in *Optical Fiber Communication Conference* (OFC, 2015), paper Tu2G.5.
3. C.-H. Yeh, H.-Y. Chen, C.-W. Chow, and Y.-L. Liu, "Utilization of multi-band OFDM modulation to increase traffic rate of phosphor-LED wireless VLC," Opt. Express **23**(2), 1133–1138 (2015).
4. C. Chen, W.-D. Zhong, and D. H. Wu, "On the coverage of multiple-input multiple-output visible light communications [Invited]," J. Opt. Commun. Netw. **9**(9), D31–D41 (2017).
5. H. Minh, D. O'Brien, G. Faulkner, L. Zeng, K. Lee, D. Jung, Y. Oh, and E. Won, "100-Mb/s NRZ visible light communications using a post-equalized white LED," IEEE Photonics Technol. Lett. **21**(15), 1063–1065 (2009).
6. L. Dai, B. Wang, Y. Yuan, S. Han, C. I, and Z. Wang, "Non-orthogonal multiple access for 5G: solutions, challenges, opportunities, and future research trends," IEEE Commun. Mag. **53**(9), 74–81 (2015).
7. H. Marshoud, V. M. Kapinas, G. K. Karagiannidis, and S. Muhaidat, "Non-orthogonal multiple access for visible light communications," IEEE Photonics Technol. Lett. **28**(1), 51–54 (2016).
8. L. Yin, W. O. Popoola, X. Wu, and H. Haas, "Performance evaluation of non-orthogonal multiple access in visible light communication," IEEE Trans. Commun. **64**(12), 5162–5175 (2016).
9. H. Marshoud, P. Sofotasios, S. Muhaidat, G. K. Karagiannidis, and B. S. Sharif, "On the performance of visible light communication systems with non-orthogonal multiple access," IEEE Trans. Wireless Commun. **16**(10), 6350–6364 (2017).
10. X. Zhang, Q. Gao, C. Gong, and Z. Xu, "User grouping and power allocation for NOMA visible light communication multi-cell networks," IEEE Commun. Lett. **21**(4), 777–780 (2017).
11. B. Lin, W. Ye, X. Tang, and Z. Ghassemlooy, "Experimental demonstration of bidirectional NOMA-OFDMA visible light communications," Opt. Express **25**(4), 4348–4355 (2017).
12. H. Li, Z. Huang, Y. Xiao, S. Zhan, and Y. Ji, "Solution for error propagation in a NOMA based VLC network: symmetric superposition coding," Opt. Express **25**(24), 29856–29863 (2017).

13. C. Chen, W.-D. Zhong, H. L. Yang, P. F. Du, and Y. B. Yang, “Flexible-rate SIC-free NOMA for downlink VLC based on constellation partitioning coding,” to appear in IEEE Wireless Commun. Lett., DOI: 10.1109/LWC.2018.2879924 (2018).
14. C. Chen, W.-D. Zhong, H. Yang, and P. Du, “On the performance of MIMO-NOMA based visible light communication systems,” IEEE Photonics Technol. Lett. **30**(4), 307–310 (2018).
15. G. Pan, J. Ye, and Z. Ding, “On secure VLC systems with spatially random terminals,” IEEE Commun. Lett. **21**(3), 492–495 (2017).
16. L. Yin and H. Haas, “Physical-layer security in multiuser visible light communication networks,” IEEE J. Sel. Areas Commun. **36**(1), 162–174 (2018).
17. Y. Liu, K. Liang, H.-Y. Chen, L.-Y. Wei, C.-W. Hsu, C.-W. Chow, and C.-H. Yeh, “Light encryption scheme using light-emitting diode and camera image sensor,” IEEE Photonics J. **8**(1), 7801107 (2016).
18. C.-W. Chow, R.-J. Shiu, Y.-C. Liu, C.-H. Yeh, X.-L. Liao, K.-H. Lin, Y.-C. Wang, and Y.-Y. Chen, “Secure mobile-phone based visible light communications with different noise-ratio light-panel,” IEEE Photonics J. **10**(2), 7902806 (2018).
19. Y. Al-Moliki, M. Alresheedi, and Y. Al-Harthi, “Physical-layer security against known/chosen plaintext attacks for OFDM-based VLC system,” IEEE Commun. Lett. **21**(12), 2606–2609 (2017).
20. B. Chen, L. Zhang, and H. Lu, “High security differential chaos-based modulation with channel scrambling for WDM-aided VLC system,” IEEE Photonics J. **8**(5), 7804513 (2016).
21. Z. Ghassemlooy, S. Arnon, M. Uysal, Z. Y. Xu, and J. Cheng, “Emerging optical wireless communications-advances and challenges,” IEEE J. Sel. Areas Commun. **33**(9), 1738–1749 (2015).
22. K. Wang, A. Nirmalathas, C. Lim, and E. Skafidas, “High-speed duplex optical wireless communication system for indoor personal area networks,” Opt. Express **18**(24), 25199–25216 (2010).
23. F. Chiarello, L. Ursini, and M. Santagiustina, “Securing wireless infrared communications through optical chaos,” IEEE Photonics Technol. Lett. **23**(9), 564–566 (2011).
24. Q. Zhang, L. Guo, and X. Wei, “Image encryption using DNA addition combining with chaotic maps,” Math. Comput. Model. **52**(11), 2028–2035 (2010).
25. X. Wang and C. Liu, “A novel and effective image encryption algorithm based on chaos and DNA encoding,” Multimed. Tools Appl. **76**(5), 6229–6245 (2017).
26. W. Zhang, C. F. 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. **35**(9), 1524–1530 (2017).
27. C. Chen, W.-D. Zhong, and D. H. Wu, “Indoor OFDM visible light communications employing adaptive digital pre-frequency domain equalization,” in *Conference on Lasers and Electro-Optics* (CLEO, 2016), paper JTh2A.118.
28. IEEE Computer Society, IEEE standard for binary floating-point arithmetic, ANSI/IEEE Std.754-1985 (1985).