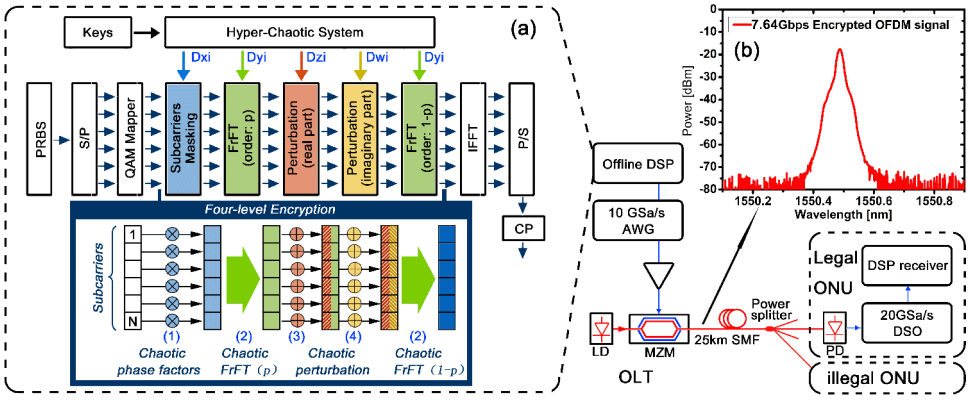
IEEE Photonics Journal
An IEEE Photonics Society Publication

Open Access

Enhanced Secure Strategy for OFDM-PON System by Using Hyperchaotic System and Fractional Fourier Transformation

Volume 6, Number 6, December 2014

M. Cheng
L. Deng
X. Wang
H. Li
M. Tang, Senior Member, IEEE
C. Ke
P. Shum, Senior Member, IEEE
D. Liu



The schematic and the experimental setup of the four-level secure OFDM-PON system.

DOI: 10.1109/JPHOT.2014.2363427
1943-0655 © 2014 IEEE

IEEE photonics SOCIETY

IEEE

Enhanced Secure Strategy for OFDM-PON System by Using Hyperchaotic System and Fractional Fourier Transformation

M. Cheng,[1] L. Deng,[1] X. Wang,[1] H. Li,[1] M. Tang,[1] *Senior Member, IEEE*, C. Ke,[1] P. Shum,[2] *Senior Member, IEEE*, and D. Liu[1]

[1]Next Generation Internet Access National Engineering Laboratory (NGIA), School of Optoelectronic Science and Engineering, Huazhong University of Science and Technology, Wuhan 430074, China
[2]School of Electrical and Electronic Engineering, College of Engineering, Nanyang Technological University, Singapore 639798

DOI: 10.1109/JPHOT.2014.2363427

Manuscript received September 10, 2014; revised October 9, 2014; accepted October 9, 2014. Date of publication October 14, 2014; date of current version October 23, 2014. This work was supported in part by the National 863 Program of China under Grant 2013AA013402 and Grant 2013AA013403, by the Fundamental Research Funds for the Central Universities HUST under Grant CXY12M005 and Grant 2013TS049, and by the National Natural Science Foundation of China under Grant 61307091 and Grant 61331010. Corresponding author: L. Deng (e-mail: denglei_hust@hust.edu.cn).

Abstract: We propose and experimentally demonstrate a scheme whereby hyperchaos and fractional Fourier transform (FrFT) techniques are integrated in an orthogonal frequency-division multiplexing (OFDM) passive optical network system. In our experiment, both security issues and transmission performance are investigated under an overall frame, and 7.64-Gb/s 16-quadrature-amplitude-modulation OFDM data with a four-level encryption scheme are successfully transmitted over a 25-km standard single-mode fiber. The results show that the system security and the transmission performance can be improved simultaneously. Moreover, the proposed scheme allows a flexible adjustment between the safety and the transmission performance according to the actual requirements.

Index Terms: Orthogonal frequency division multiplexing (OFDM), passive optical network (PON), fractional Fourier transform (FrFT), chaos, optical communication.

1. Introduction

Passive optical networks (PONs) have attracted considerable attention owing to their superiorities, such as cost effectiveness, energy savings and relatively high signal transmission capability [1], [2]. Moreover, the orthogonal frequency division multiplexing passive optical network (OFDM-PON) has emerged as one of the most promising solutions to meet the requirement of next generation networks due to its high spectral efficiency, flexibility to arbitrary modulation constellations, high tolerance to fiber dispersion [3]–[5]. The growing attractiveness of such technique has put a demand for greater security for reliable data transmission at the physical layer. Many secure strategies in PON systems are proposed in form of cryptographic and authentication protocols at the media access control (MAC) layer or higher layers [6], [7]. However, the physical layer of the PON system is more susceptible to malicious attacks [8].

Various techniques which secure the PON systems at the physical layer have been explored recently [9]–[15]. Among these proposed technologies, optical chaos based scheme have garnered much attention in the last decade. It has been confirmed that high speed secure communication can be achieved in wavelength division multiplexing (WDM) PONs by adopting optical chaos [10]. However the main problem of optical chaos system is that the parameter space dimension is restricted by the physical devices [16]. To circumvent this drawback, digital keys have been introduced into the chaotic communication systems [16]–[18], as a result, the key space is greatly enlarged. On the other hand, digital chaotic systems with large key space dimension which is implemented by using the digital signal processor (DSP) are adopted to enhance the security of OFDM-PON systems. These methods including chaotic mask [11], [12] and chaotic scrambling [13]–[15] are proved to be the effect strategy in OFDM-PON due to its high initial condition and parameter sensitivity. More important, digital chaos based methods are especially attractive for OFDM-PON due to the fact that OFDM-PON has flexible OFDM subcarriers and time slots which both could be easily adjusted on the DSP. It is worth noting that when comes to the secure communication systems, most concerns are focused only on the safety issues. The security and transmission performance are usually considered as separate and non-associate parts in the existing researches. However, the encryption schemes implemented at the physical layer will affect the transmission performance unavoidably, and efforts should be made to control such influence to a benign direction. In our scheme, these two important aspects are investigated simultaneously under an overall frame.

In this paper, we propose and experimentally demonstrate an enhanced secure strategy for OFDM-PON system by adopting hyper chaos and Fractional Fourier transformation (FrFT) techniques. The most important aspect in a chaos-based secure system is the complexity of the chaotic source, and the Lyapunov exponent is used as a quantifier of the initial value sensitivity and complexity of a chaos system. For regular chaotic systems, there is only one positive Lyapunov exponent. The hyper-chaotic system with high dimensional characteristic and more than one positive Lyapunov exponent may be a good candidate for enhancing the complexity of the masking signal [19]. On the other hand, FrFT is a generalization of the Fourier transform, and can be seen as the projection of a given signal between time and frequency axis. This technique has been widely used in signal processing, secure communication and image encryption [20]–[23]. Combining these two techniques will introduce additional degrees of freedom to enhance the security of the system. More importantly, we found that the transmission performance of the proposed OFDM-PON system can also been improved. Both the security and transmission requirements have been satisfied simultaneously in our scheme. The proposed scheme also allows a flexible adjustment between safety and transmission performance according to the actual requirements.

2. Principle

A four-dimensional (4-D) hyper-chaotic system is utilized to generate hyper-chaotic sequences which are then used in a four-level encryption. The proposed schematic is illustrated in Fig. 1(a). At the transmitter, a data stream is mapped onto quadrature-amplitude-modulation (QAM) subcarriers after serial-to-parallel (S/P) converting. Subsequently, the OFDM subcarriers are masked by phase factors which are chaotically generated in the first level encryption. The second level encryption is split into two parts: two FrFT operations of fractional order p and $1 - p$ respectively with the parameter p controlled by the chaotic sequences. The third and fourth level encryptions are performed between these two parts: the subcarriers are perturbed chaotically both in the real part and in the imaginary part. The chaotic sequences are generated by a hyper-chaotic system [19] as expressed in

$$\begin{cases} \dot{x} = -yz + ax \\ \dot{y} = xz + by \\ \dot{z} = \left(\frac{1}{3}\right)xy + cz + 0.2w \\ \dot{w} = dx + 0.5yz + 0.05w. \end{cases} \tag{1}$$

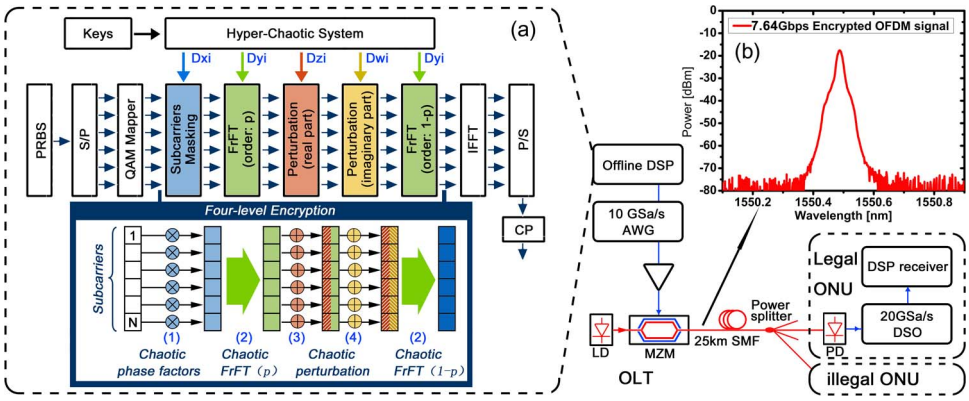


Fig. 1. The schematic and the experimental setup of the four-level secure OFDM-PON system.

where a, b, c, and d are parameters. According to the literature [19], with $a = 5.0$, $b = -10.0$, $c = -3.8$, and $d \in [0, 1.3]$, this system behaves a chaotic or hyper-chaotic characteristic. The differential equations in (1) are solved by 4th-order Runge-Kutta method and the time step size k is chosen as 0.001 here. The generated 4-D sequences $\{x_i\}$, $\{y_i\}$, $\{z_i\}$, and $\{w_i\}$ are then post processed as described in

$$\begin{aligned} D_{xi} &= \mathrm{mod}\left(Extract(x_i, 12, 13, 14), 256\right)/256 \\ D_{yi} &= \mathrm{mod}\left(Extract(y_i, 12, 13, 14), 256\right)/256 \\ D_{zi} &= \mathrm{mod}\left(Extract(z_i, 12, 13, 14), 256\right)/128 - 1 \\ D_{wi} &= \mathrm{mod}\left(Extract(w_i, 12, 13, 14), 256\right)/128 - 1 \end{aligned} \tag{2}$$

where the function $Extract(\alpha, m, n, r)$ returns an integer which is constructed by the mth, nth and rth digits in the decimal part of α. Then, $\{D_{xi}\}$ is used as the phase factors for OFDM subcarriers masking. After the first level of encryption, the generated data symbol S'_k could be written as

$$S'_k = S_k \cdot e^{jD_{xk} \cdot 2\pi}, (1 \le k \le N) \tag{3}$$

where S_k is the data symbol on kth subcarrier before the chaotic masking, and N is the total number of subcarriers. Subsequently, the second, third and fourth levels of encryption are performed. The generated time domain OFDM signal $x(t)$ after IFFT could be expressed as

$$x(t) = \frac{1}{\sqrt{N}} \sum_{n=1}^{N} F^{1-p}\left[F^p(S'_n) + M(D_{zi} + jD_{wi})\right] \cdot e^{j(2\pi n \Delta f t)}, (0 \le t < NT) \tag{4}$$

where Δf is the subcarrier spacing and NT is the symbol period. M is defined as the perturbation amplitude, here, we chose $M = 4$. $F^p(S'_n)$ denotes the data symbol on nth subcarrier after FrFT with order p.

The FrFT operator F^p can be viewed as a change in the representation of a signal corresponding to a $p\pi/2$ counterclockwise axis rotation, and it is defined by

$$\begin{aligned} S^p(u) &= F^p\{s(t)\}(u) \\ &= \sqrt{1 - \frac{j}{\tan\left(p\frac{\pi}{2}\right)}} \int_{-\infty}^{\infty} s(t) e^{j\pi\left[(u^2+t^2)\cot\left(p\frac{\pi}{2}\right) - 2ut\csc\left(p\frac{\pi}{2}\right)\right]} dt \end{aligned} \tag{5}$$

where, $S^p(u)$ is the fractional Fourier transformation of $s(t)$, and p is a real number known as the FrFT order.

The parameter p is different in each OFDM frames and directly controlled by the chaotic sequence $\{D_{yi}\}$. Under the four-level encryption, the fractional order p and the chaotic sequences are interlocked together, so the original chaotic sequences are unacquirable without knowing the current p, and if an eavesdropper can only get the transmitted signal, the individual will not be able to crack the FrFT parameters without the information of chaotic sequences. The four levels of encryption which perform a mutual cover eventually enhance the system security.

The key space is a major concern in designing the secure communication systems, a large key space is necessary for resisting the exhaustive attack. Thanks to the high dimensional property of the hyper-chaos system, the key space could be large enough in the proposed scheme. The main part of the key space can be formed by the initial values of (1). Each of the initial values could have a bit length of 64-bit, and consider the fact that the range of these initial values is restricted by the shape of chaos attractor, we only count the decimal part (56 bit) for a conservative estimate, and the size could be about 10^{67} $(2^{56} \times 2^{56} \times 2^{56} \times 2^{56} \approx 10^{67})$. Except for the initial values of the chaos system, the parameter d can also be used as safe key, so the total size of the key space could beyond 10^{67}.

In the proposed scheme, the complexity of hyper-chaos operations including the chaotic subcarrier distortion in level 1 and chaotic perturbation in levels 3 and 4 are proportional to N. The complexity of FrFT operations with order p and $1 - p$ in level 2 are $N \times \log_2 N$ [24]. As a result, there is additional processing latency compared with the conventional OFDM scheme. The FrFT point size cannot be too large due to the restriction of the hardware processing ability at the ONU, and a size of 128 is enough to guarantee both the calculation complexity and security.

3. Experiment Setup

The experimental setup of our scheme is shown in Fig. 1. At the OLT, the downstream binary sequence with a PRBS length of $2^{15} - 1$ is mapped onto 257 subcarriers, of which 128 subcarriers carry real 16-QAM data and one is unfilled DC subcarrier. The remaining 128 subcarriers are the complex conjugate of the aforementioned 128 subcarriers. The Hermitian symmetry [25] is utilized for IFFT in order to perform the direct intensity modulation. The cyclic prefix is 1/10 of the IFFT length (512 point), which means that the OFDM symbol size is 563. Training symbol is inserted at the beginning of each frame that contains 9 data symbols. An arbitrary waveform generator (AWG, AWG7122B) with a sample rate of 10 GSa/s is used to generate the OFDM signal with a raw data rate of 8.18 Gbps $(10\ \text{GSa/s} \times 4 \times 128/563 \times 9/10)$. For the net data rate, 7% FEC overhead needs to be considered, so the net data rate is 7.64 Gb/s. A 100 kHz-linewidth continuous-wave (CW) external cavity laser (ECL, $\lambda_1 = 1550.488$ nm) is used as optical source. The encrypted OFDM signal is modulated onto the optical carrier by a Mach-Zehnder modulator (MZM) which is working in the linear region, and the optical spectrum of the encrypted OFDM signal is shown in Fig. 1(b). After 25 km standard single mode fiber (SSMF) transmission, the signal is captured by a 4 GHz photodiode (PD) and a 20 GSa/s digital sampling oscilloscope (DSO) (Tektronix, CSA7404B). Offline signal decryption, demodulation and BER testing are then performed by the DSP, and 65536 bits are calculated for BER tester in our experiment.

4. Experiment Results and Discussions

4.1. Main Results

The complementary cumulative distribution function (CCDF) of the PAPR of the OFDM signal with encryption and the conventional OFDM signal are shown in Fig. 2. It is obvious that the OFDM signal without encryption has larger PAPR than the encrypted one, and the difference at the probability of 10^{-4} is about 1.8 dB. Fig. 3 shows the measured BER curves, for the encrypted 16QAM-OFDM signal with correct decryption, the data can be recovered with a transmission penalty of 0.3 dB at the forward error correction (FEC) limit (BER of 3.8×10^{-3}) before

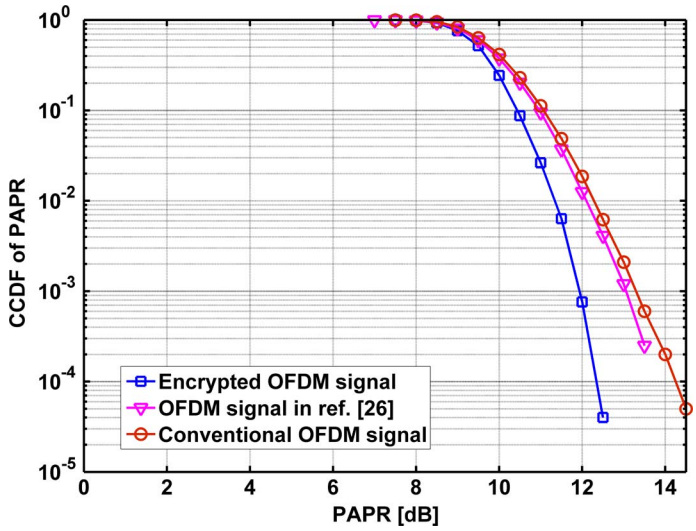


Fig. 2. CCDF of PAPR for the encrypted OFDM signal compared with the conventional OFDM scheme and the scheme proposed in [26].

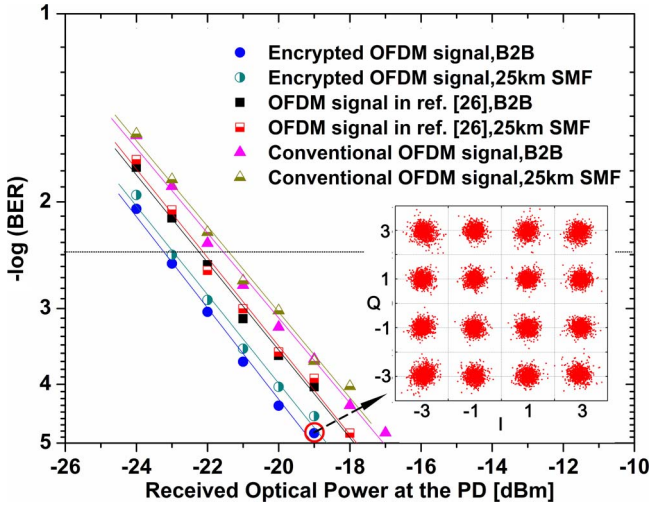


Fig. 3. BER curves of encrypted OFDM signal compare with the conventional OFDM scheme and the scheme proposed in [26].

and after 25 km SSMF transmission. On the other hand, the performance of traditional OFDM signal (without encryption) is degraded by about 1.8 dB compared with the encrypted case.

Moreover, we have compare the PAPR and the BER performance of the scheme with our previous proposed method in [26]. Although the encryption algorithm in [26] is different from the current method, its system structure is similar to the current scheme from signal transmission point of view. As can be seen in Fig. 2, the PAPR of the OFDM signal in [26] at the probability of 10^{-4} is about 0.5 dB better than the conventional OFDM signal and about 1.3 dB worse than our current encryption scheme. And the BER performance of the scheme in [26] is better than the conventional OFDM and worse than the current one, as shown in Fig. 3. This phenomenon could be attributed to the following two facts: First, the chaotic subcarrier mask acts as random interleave [14], and the original data is disrupted by the noise-like chaotic sequence, so that the correlation between the original data bits is weakened after interleaving. By this way, the impact of the data burst errors could be reduced, thus the transmission quality and system reliability

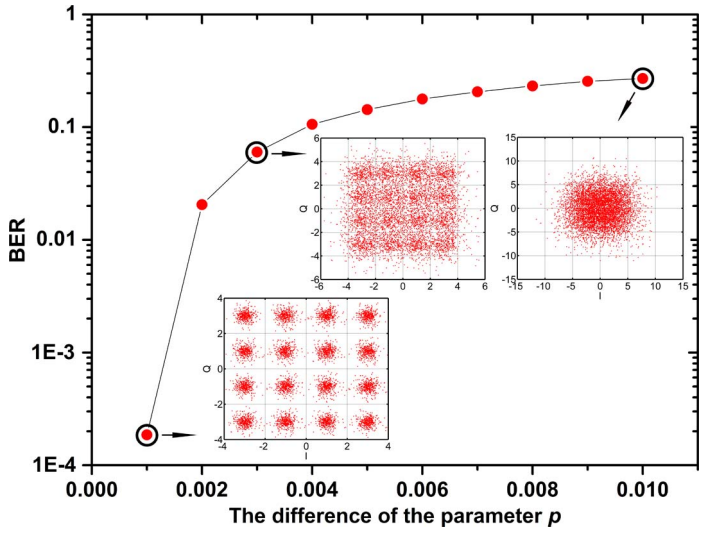


Fig. 4. Sensitive dependence on the fractional order.

can be improved. Second, the PAPR of the transmitted OFDM signal is decreased due to the FrFT operation. The transmission performance is affected by the PAPR due to nonlinearity of network components such as electrical amplifier and optical modulator.

Sensitive dependence on secret keys is a important indicator for the security of an encryption system. Chaotic sequences are very sensitive to their initial values and parameters, since it is the basic feature of chaos. The sensitivity of the OFDM-PON system with respect to chaos has also been studied in literatures [11]–[15]. Therefore, we focus on the sensitive dependence on the FrFT order here. Fig. 4 shows the BER performance when the receiver has different p with the transmitter when other decryption vectors (the phase factors in level 1 and the perturbation vector in levels 3 and 4, respectively) remain correct. The results indicate that the performance is significantly deteriorated when the difference of p is bigger than 0.003. The corresponding constellations are shown in the insets of Fig. 4.

4.2. Detailed Discussions

The results in Section 4.1 indicate that the security performance and transmission performance can be improved simultaneously in our scheme. Moreover, by detailed investigation, we found that both the security and the PAPR are significantly affected by the perturbation amplitude M, which indicate that this parameter plays a key role in the proposed method.

Fig. 5 shows the CCDF of the PAPR of the OFDM signal with varying M. It is clearly observed that the PAPR of the encrypted OFDM signal is reduced when we decrease the perturbation amplitude M. As described in Section 4.1, low PAPR could lead to certain degree of transmission performance improvement. On the other hand, as shown in Fig. 6, if we decrease M, the sensitivity to the FrFT order p will also decrease. Fig. 7 shows the BER for wrong decryption keys versus M, when M is large, the BER for the illegal receiver is about 0.489, which means a good performance of encryption. When M is small, the BER for the illegal receiver is reduced accordingly, which indicates a certain degree of encryption performance degradation. This could be attributed to the fact that the sensitivity of the FrFT order is degraded.

The discussions mentioned above mean that the PAPR can be further improved by decreasing the perturbation amplitude, meanwhile certain degree of safety performance is sacrificed. This indicates that our scheme allows a flexible adjustment between safety and transmission performance according to the actual requirements. However, when further decreasing the PAPR, the transmission performance will not have a remarkable improvement. This is because in a short distance communication, i.e., in a PON system, when the PAPR is very large, the

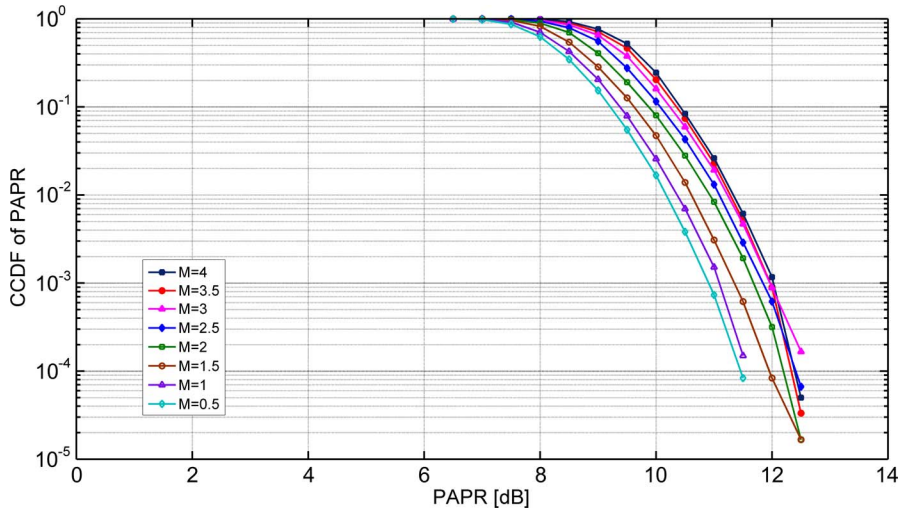


Fig. 5. CCDF of PAPR for the encrypted OFDM signal with different perturbation amplitude *M*.

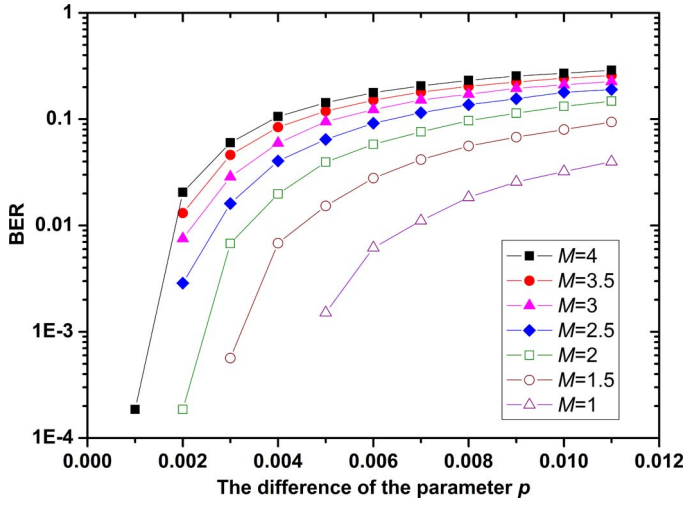


Fig. 6. Sensitive dependence on the fractional order with different perturbation amplitude *M*.

transmission performance is affected mainly by the nonlinearity of the devices, and when PAPR is relatively small, the channel noise will be the major factor of performance degradation. Nevertheless, in long distance communication schemes, the fiber nonlinear effect induced by high PAPR plays a more important role, while such effect may be neglected in short range schemes. Thus indicate that the proposed method may also be beneficial to long distance OFDM communication schemes which will be investigated in our following works.

5. Conclusion

We have proposed an enhanced secure strategy for OFDM-PON by adopting hyper-chaotic system and FrFT technique. Four levels of encryption are controlled by a 4-D hyper-chaotic system. By this way, the system security and the transmission performance are improved simultaneously. 7.64 Gbps encrypted 16QAM-OFDM signal is successfully transmitted over 25 km SSMF in our experiment. Compared with the conventional OFDM signal, the PAPR of the encrypted OFDM signal is decreased by about 1.8 dB due to the FrFT operation when the perturbation amplitude

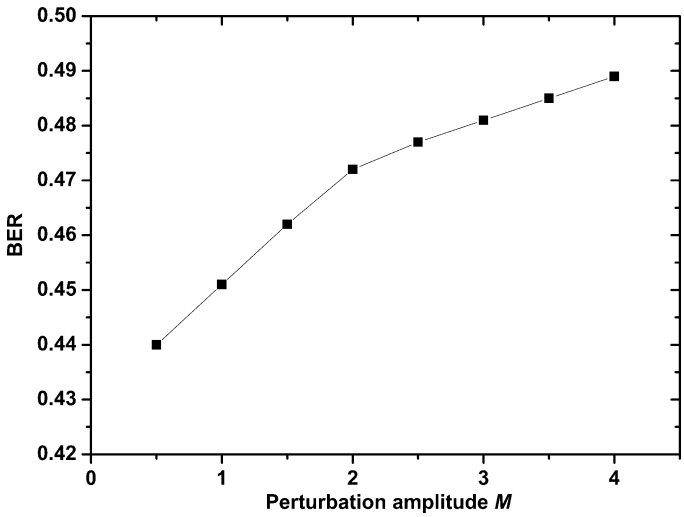


Fig. 7. BER for wrong decryption keys under different perturbation amplitude M.

$M = 4$, and the transmission performance is improved by about 1.8 dB. The results also show that the proposed scheme is sensitive to the FrFT order, which indicate that the FrFT plays a key role in improving both the security and the transmission performance. Last but not the least, the proposed scheme allows a flexible adjustment between safety and transmission performance according to the actual requirements by setting the proper perturbation amplitude. This security enhanced OFDM-PON scheme has potential applications in future secure communications at the physical layer.

References

[1] J. 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] 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] N. Cvijetic *et al.*, "Terabit optical access networks based on WDM-OFDMA-PON," *J. Lightw. Technol.*, vol. 30, no. 4, pp. 493–503, Feb. 2012.
[5] J. Yu, M.-F. Huang, D. Qian, L. Chen, and G.-K. Chang, "Centralized lightwave WDM-PON employing 16-QAM intensity modulated OFDM downstream and OOK modulated upstream signals," *IEEE Photon. Technol. Lett.*, vol. 20, no. 18, pp. 1545–1547, Sep. 2008.
[6] 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.
[7] M. Hossen, K. D. Kim, and Y. Park, "Synchronized latency secured MAC protocol for PON based large sensor network," presented at the 12th ICACT, Phoenix Park, Korea, 2010, 1528–1532.
[8] K. Shaneman and S. Gray, "Optical network security: technical analysis of fiber tapping mechanisms and methods for detection & prevention," presented at the IEEE MILCOM, Monterey, CA, 2004, 711–716.
[9] P. Cao, X. Hu, J. Wu, L. Zhang, 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. ID. 7901006.
[10] N. Jiang, D. Liu, C. Zhang, and K. Qiu, "Modeling and simulation of chaos-based security-enhanced WDM-PON," *IEEE Photon. Technol. Lett.*, vol. 25, no. 19, pp. 1912–1915, Oct. 2013.
[11] B. Liu, L. Zhang, X. Xin, and J. Yu, "Constellation-masked secure communication technique for OFDM-PON," *Opt. Exp.*, vol. 20, no. 22, pp. 25161–25168, Oct. 2012.
[12] L. Zhang, B. Liu, X. Xin, and D. Liu, "A novel 3D constellation-masked method for physical security in hierarchical OFDMA system," *Opt. Exp.*, vol. 21, no. 13, pp. 15627–15633, Jun. 2013.
[13] B. Liu, L. Zhang, X. Xin, and J. Yu, "Physical layer security in CO-OFDM transmission system using chaotic scrambling," *Opt. Commun.*, vol. 291, pp. 79–86, Nov. 2012.
[14] L. Zhang, X. Xin, B. Liu, and J. Yu, "Physical-enhanced secure strategy in an OFDM-PON," *Opt. Exp.*, vol. 20, no. 3, pp. 2255–2265, Jan. 2012.
[15] 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.

[16] R. M. Nguimdo, P. Colet, L. Larger, and L. Pesquera, "Digital key for chaos communication performing time delay concealment," *Phys. Rev. Lett.*, vol. 107, no. 3, p. 034103, Jul. 2011.
[17] R. M. Nguimdo and P. Colet, "Electro-optic phase chaos systems with an internal variable and a digital key," *Opt. Exp.*, vol. 20, no. 23, pp. 25333–25344, Oct. 2012.
[18] R. Lavrov, M. Jacquot, and L. Larger, "Nonlocal nonlinear electro-optic phase dynamics demonstrating 10 Gb/s Chaos Communications," *IEEE J. Quantum Electron.*, vol. 46, no. 10, pp. 1430–1435, Oct. 2010.
[19] C. H. Chen *et al.* "A new hyper-chaotic system and its synchronization," *Nonlinear Anal.: Real World Appl.*, vol. 10, no. 4, pp. 2088–2096, Aug. 2009.
[20] M. Cheng, L. Deng, H. Li, and D. Liu, "Enhanced secure strategy for electro-optic chaotic systems with delayed dynamics by using fractional Fourier transformation," *Opt. Exp.*, vol. 22, no. 5, pp. 5241–5251, Feb. 2014.
[21] B. Hennelly and J. T. Sheridan, "Optical image encryption by random shifting in fractional Fourier domains," *Opt. Lett.*, vol. 28, no. 4, pp. 269–271, Feb. 2003.
[22] Q. Ran, H. Zhang, J. Zhang, L. Tan, and J. Ma, "Deficiencies of the cryptography based on multiple-parameter fractional Fourier transform," *Opt. Lett.*, vol. 34, no. 11 pp. 1729–1731, Jun. 2009.
[23] M. Joshi, Chandrashakher, and K. Singh, "Color image encryption and decryption using fractional Fourier transform," *Opt. Commun.*, vol. 279, no. 1 pp. 35–42, Jul. 2007.
[24] S. C. Pei and J. J. Ding, "Closed-form discrete fractional and affine Fourier transforms," *IEEE Trans. Signal Process.*, vol. 48, no. 5, pp. 1338–1353, May 2000.
[25] R. P. Giddings *et al.*, "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. Exp.*, vol. 18, no. 6, pp. 5541–5555, Mar. 2010.
[26] L. Deng *et al.*, "Secure OFDM-PON system based on chaos and fractional Fourier transform techniques," *IEEE J. Lightw. Technol.*, vol. 32, no. 15, pp. 2629–2635, Jun. 2014.