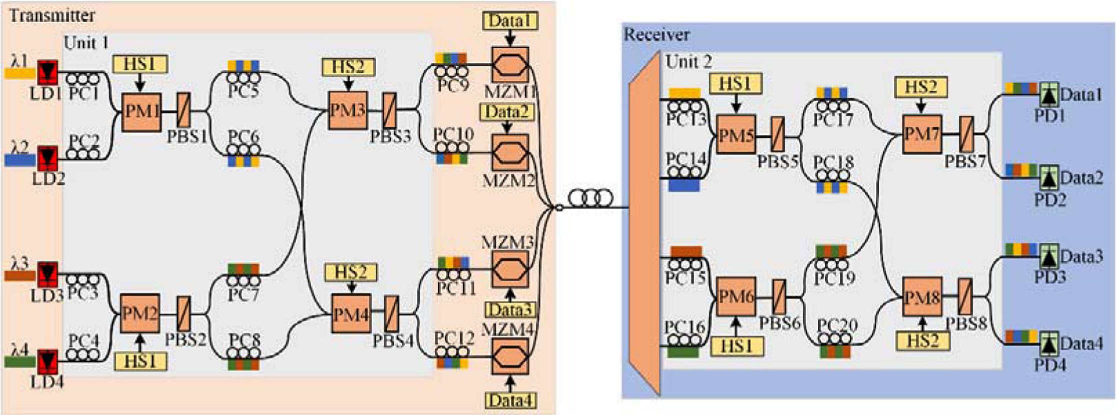
IEEE Photonics Journal
An IEEE Photonics Society Publication

Open Access

# A Novel Optical Frequency-Hopping Scheme Based on a Flexible Structure for Secure Optical Communications

Volume 11, Number 1, February 2019

De Chao Ban
Qing Chao Huang
Yin Fang Chen
Yi Chao Qi
Wei Chen
Ning Hua Zhu, *Member, IEEE*



DOI: 10.1109/JPHOT.2019.2895353

# A Novel Optical Frequency-Hopping Scheme Based on a Flexible Structure for Secure Optical Communications

**De Chao Ban ,[1,2] Qing Chao Huang,[1,2] Yin Fang Chen ,[1]**
**Yi Chao Qi ,[1,3] Wei Chen ,[1] and Ning Hua Zhu ,[1] *Member, IEEE***

[1]State Key Laboratory of Integrated Optoelectronics, Institute of Semiconductors, Chinese Academy of Sciences, Beijing 100083, China
[2]College of Materials Science and Opto-Electronic Technology, University of Chinese Academy of Sciences, Beijing 100049, China
[3]School of Microelectronics, University of Chinese Academy of Sciences, Beijing 100049, China

*DOI:10.1109/JPHOT.2019.2895353*

Manuscript received December 11, 2018; revised January 13, 2019; accepted January 21, 2019. Date of publication January 25, 2019; date of current version February 11, 2019. This work was supported in part by the National Natural Science Foundation of China under Grant 61675196; and in part by the Strategic Leading Science and Technology Program of Chinese Academy of Sciences (CAS) under Grant XDA06010305. Corresponding author: W. Chen (e-mail: wchen@semi.ac.cn).

**Abstract:** A novel optical frequency-hopping scheme based on a flexible structure for secure optical communications is proposed and demonstrated. In the proposed scheme, critical users' data are divided into a lot of segments, and these segments are transmitted by different optical wavelengths in time domain. In other words, one channel optical carrier carries different users' data segments. A flexible structure was demonstrated and used in optical frequency-hopping system to simplify the structure and decrease the cost of the security system. In this paper, the viability of a four-wavelength-frequency-hopping secure optical communication system with a 25-Gb/s error-free transmission through a 32-km single-mode fiber and a 8-km dispersion compensation fiber was demonstrated and verified by simulation tools.

**Index Terms:** Optical frequency hopping, communication system security, optical communication networks.

## 1. Introduction

With the increasing capacity of optical communication due to the development of wavelength division multiplexing (WDM) technology, modern societies are becoming increasingly dependent on communication networks. Meanwhile, with the growing demand for protecting personal privacy on the Internet, it is important to enhance the security of optical network. Optical network is vulnerable to be attacked at the physical layer by the means of fiber bending, splitting, evanescent coupling, scattering, and V-grooves [1], [2]. Therefore, it is necessary to increase the security of optical networks at physical layer. In stealth transmission communication technology, a user's signal is spread in a dedicated secure channel which is overlaid onto a public channel in an existing fiber link [3]. The user's data are encoded and become a noise-like signal. Thus, user's signal is difficult to be detected and intercepted. However, this technology needs to add an additional security channel which would make communication system more complex. In [4], [5], chaotic communication systems are

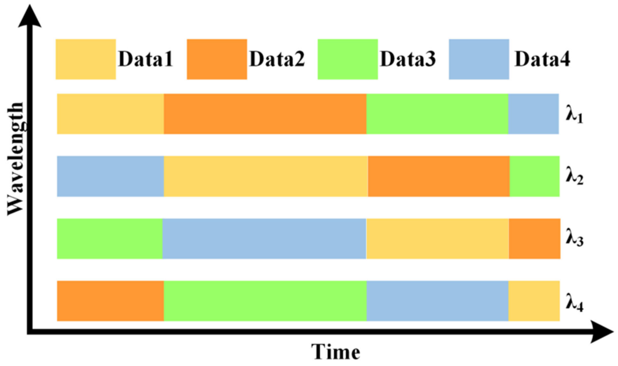


Fig. 1. Scheme of optical frequency-hopping.

demonstrated to enhance the security of optical network. Whereas its encrypted signals are analog, the transmission distance would be restricted in fiber communication system. Optical code-division multiplexing-access (OCDMA) technology [6], [7] has been discussed for implementing physical-layer security of communication system, but it has the same drawback as chaotic communication systems. In addition, a research has demonstrated that user data can be eavesdropped by energy detectors in an on-off keying (OOK) system [8].

Optical frequency-hopping is another physical layer technique which is applied to protect user data from being eavesdropped effectively [9], [10]. In an optical frequency hopping system, a user's signal hops among N optical channels rapidly and randomly in time domain. As show in Fig. 1, the data from one user would be modulated onto different optical carriers at different time slots. Without knowing the hopping pattern, it's extremely difficult for the eavesdropper to recover the data from data segments. A "passive hopping" scheme in wavelength-division multiplexing (WDM) system had been demonstrated [9]. In that proposed system, signals hopped among different channels rapidly with the control of a field-programmable gate array (FPGA) chip. The hopping rate which can be changed by the chip, is limited to 10-Gb/s due to the chip performance. In [11], an optical frequency-hopping scheme based on optical frequency shift keying (OFSK) had been discussed. That proposed two-frequency-hopping system supported 10.6-Gb/s error-free transmission through 20-km dispersion shifted fiber (DSF) and 40-km SMF. In that system, an OFSK transmitter used to generate optical frequency-hopping carriers was constituted by a delayed interferometer (DI) and a phase modulator which was driven by hopping sequence (HS). However, due to the fixed wavelength response of the DI, only some certain wavelengths can be used. In addition, in the receiver of that proposed communication system, one channel signal was decrypted by two sets of $LiNbO_3$ intensity modulators and two HS generators which made the system more complex and expensive. Another OFSK transmitter based on polarization modulation had been demonstrated, which could use continuous optical carriers and have simple structure [12]–[14].

In this paper, a novel optical frequency-hopping scheme based on flexible structures for secure optical communication is proposed and demonstrated. The communication system security is enhanced, due to the users' data are fragmented by an OFSK transmitter with the hopping sequence controlling and transmitted by more than one wavelength. The proposed secure communication system has a high hopping rate with a flexible and simple structure, meanwhile supports continuous optical carriers. The performance and feasibility of the system was investigated by VPI transmission Maker.

## 2. Principle

Fig. 2 illustrates the structure and principle of the proposed OFSK transmitter based on polarization modulation [8]. Two continuous wave (CW) optical beams ($\lambda_1$ and $\lambda_2$) are combined by a coupler and

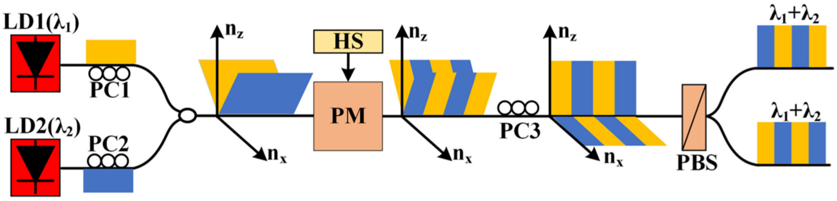


Fig. 2. OFSK transmitter and operation principle. LD: continuous wave laser diode; PC: polarization controller; HS: hopping sequence; PM: phase modulator; PBS: polarization beam splitter.

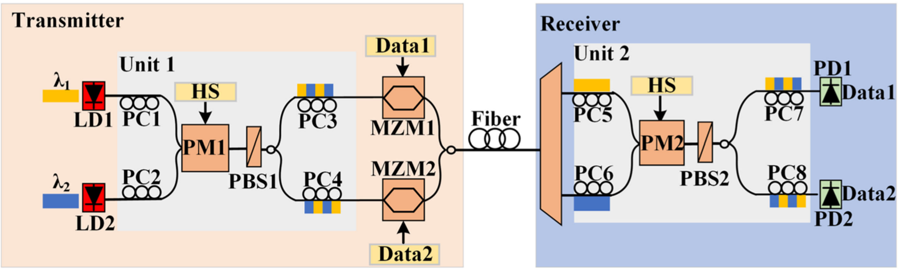


Fig. 3. Proposed optical frequency-hopping system. LD: laser diode, PC: polarization controller, PM: phase modulator, HS: hopping sequence, PBS: polarization beam splitter, MZM: Mach-Zehnder modulator, PD: photoelectric detector.

injected into an optical phase modulator (PM). Before they are injected into the PM, the polarization of each light is adjusted to be linearly polarized and orthogonal to each other by two polarization controllers (PC1 and PC2), respectively. Meanwhile, their polarizations are $\pm\pi/4$ relative to the principal axes ($n_z$) of the PM. The HS is generated by a pseudo-random binary sequence (PRBS) generator. When a ‘1’ signal is added onto the PM, a voltage $V\pi$ will apply to it. And this voltage will induce $\pi$ phase shift in the component of $n_z$ direction, but no phase shift in $n_x$ direction. Then the polarization of each beam light will rotate $\pi/2$, that is to say, when a ‘1’ signal is added onto the PM, $\lambda_1$ and $\lambda_2$ will exchange their polarization states. When a ‘0’ signal is added onto PM, no phase shift is induced both in the component of $n_z$ direction and $n_x$ direction due to no voltage is applied to PM, thus the polarization of two beam lights will keep invariable. As a consequence, two OFSK signals are acquired and the wavelengths of two OFSK signals are complementary in time domain. Then the polarization components of two OFSK signals are adjusted to be 0 and $\pi/2$ relative to the $n_z$ direction of PM by PC3. In order to divide these two complementary optical carriers, a polarization beam splitter (PBS) is used behind PC3. Finally, using this OFSK transmitter, two constant intensity, complementary OFSK signals are generated. In the proposed secure scheme, the hopping rate is same as the modulation rate of PM.

Fig. 3 shows the schematic diagram of a two-wavelength-frequency-hopping communication system, which consists of a transmitter and a receiver. The transmitter is constituted by an OFSK transmitter and two data modulators. In this optical frequency-hopping communication system, an OFSK transmitter generate two OFSK signals which are used to be optical carriers and two channels user data are modulated onto them, respectively. Then these two carriers are combined and fed into a SMF by a coupler. In the receiver of this proposed secure system, signals in fiber are divided into two wavelengths with $\lambda_1$ and $\lambda_2$ by a demultiplexer and fed into unit 2. The polarization states of two beams are adjusted to be linearly polarized and $\pm\pi/4$ relative to the principal axes ($n_z$) of the PM2 by two polarization controllers (PC5 and PC6), respectively. Due to the HS used on PM2 is same as the one used on PM1, optical carrier is decrypted and divided into two polarization states. Then two channel optical carriers that contain user data are acquired by using PBS2 and two polarization controllers (PC7 and PC8). In other words, this proposed secure system use the same structure

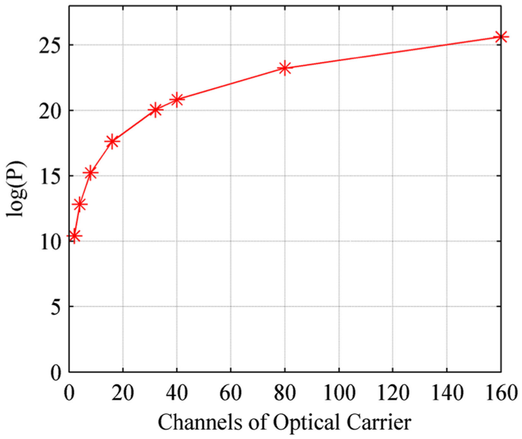


Fig. 4. Data volume versus channels of optical carriers.

(unit 1 and unit 2) to encrypt and decrypt the uses' data. Due to the same unit we can simplify the structure of optical frequency-hopping system and make it more flexible. For example, when the secure system is upgraded from two-wavelength-frequency-hopping communication system to four-wavelength-frequency-hopping communication system, just need to increase the number of units without adding additional devices. Unlike the scheme mentioned in [11], two additional Mach-Zehnder intensity modulators (MZM) and HS generators are demanded in the receiver to recover one original user data. After these processes, the user data can be recovered from encryption signals by two photoelectric detectors (PD1 and PD2).

## 3. Security Analysis

In this discussion, the security of proposed optical frequency-hopping communication system will be analyzed. Assuming that user data are constituted by units of information and the size of a unit is S bits. In addition, only an eavesdropper captures all the S bits, can he acquire a unit of integrated information. In the proposed secure system, there are N optical channels, the transmission rate is T in each channel and the hopping rate is H. If an eavesdropper wants to recover a unit of information through violent attack without knowing HS, he needs to verify all the possible combinations of the unit in a short time. The bit error rate (BER) of information captured from hacking channel is represented with E. Basing on the above analyzing, the data volume P which represents an eavesdropper needs to verify within one second can be expressed as:

$$P = ((N)^{\frac{S\cdot H}{T}})/(1-E)^{S} \cdot T = (N)^{\frac{S\cdot H}{T}} \cdot \left(\frac{1}{1-E}\right)^{S} \cdot T \tag{1}$$

In the view of mathematics, when a probability of an event is less than 0.01, it can be considered as a small probability event. Similarly, if the intercept possibility is less than 0.01, the optical frequency-hopping system can be considered as a security system. Therefore, the correctional data volume is:

$$P = (N)^{\frac{S\cdot H}{T}} \left(\frac{1}{1-\mathrm{E}}\right)^{S} \cdot 0.01T \tag{2}$$

As equation (2) shows, the security of the proposed system can be enhanced by increasing the hopping rate, and the simplest method is adding communication channels as many as possible. Assuming the size of a unit is 8 bits and the hopping rate is equal to the bit rate. As shown in Fig. 4, when there are 16 optical carrier channels are applied in this proposed frequency-hopping secure system and the bit rate is 10-Gb/s, then the data volume is $4.3 \times 10^{17}$. In other word, if an

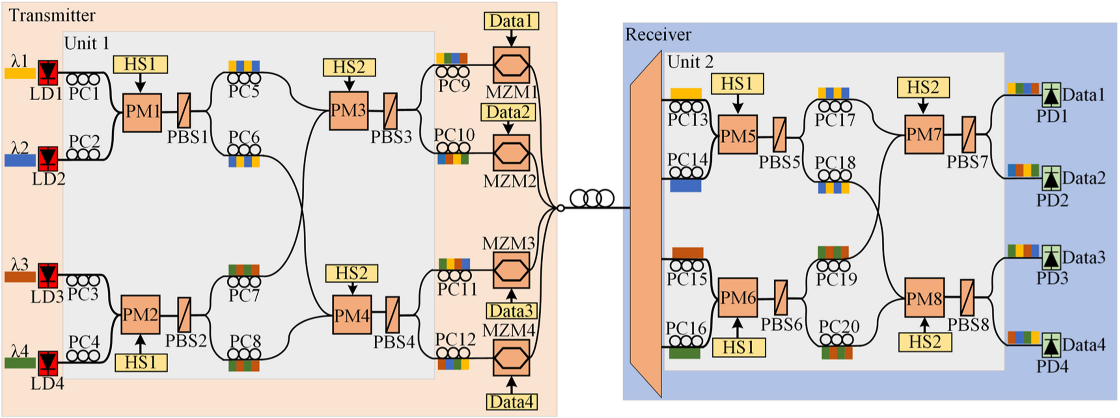


Fig. 5. Four-wavelength-frequency-hopping system. LD: laser diode, PC: polarization controller, PM: phase modulator, HS: hopping sequence, PBS: polarization beam splitter MZM: Mach-Zehnder modulator, PD: photoelectric detector.

eavesdropper attacks a communication system which has 16 channels optical carriers, then he has to process data in $4.3 \times 10^{17}$ bit/s. Such a large amount of data volume needs to be processed with the help of supercomputers. When the channels are 160 [15], the data volume is over $10^{26}$. Moreover, with the numbers of channel increasing, the system will be more security. Thus, the communication system can be proved to be security.

## 4. Simulation and Result

As shown in Fig. 5, a four-wavelength-frequency-hopping communication system has been simulated and discussed. This system is constituted by two same structures as Fig. 3 has shown, so one OFSK signal consists of four different wavelengths. That is to say, using several the same structures could realize optical carrier hopping among more than four different wavelengths. In the transmitter, the optical carrier's wavelengths are $\lambda_1 = 1553.6$ nm, $\lambda_2 = 1554.4$ nm, $\lambda_3 = 1555.2$ nm and $\lambda_4 = 1556.0$ nm, and two sets of different PRBS hopping sequence (HS1 and HS2) were used as encrypted data to drive two sets of phase modulators (PM1, PM2 and PM3, PM4), respectively. Four channels user data (Data1, Data2, Data3 and Data4) were modulated onto the four channels optical carrier by MZM1, MZM2, MZM3 and MZM4, respectively. In the receiver, optical carriers were split into four wavelengths with $\lambda_1$, $\lambda_2$, $\lambda_3$ and $\lambda_4$ by a demultiplexer. Later, $\lambda_1$ and $\lambda_2$, $\lambda_3$ and $\lambda_4$ were fed into PM5 and PM6 which were driven by HS1, respectively. Afterwards, the first channel signal from the output port of PBS5 and the third channel signals from the output port of PBS6 were fed into PM7, and the other two channels (the second and the forth) signals were fed into PM8. PM7 and PM8 were driven by HS2. Due to the different polarization states, the optical carriers were divided by PBS7 and PBS8, respectively, and four channels user data were detected by photoelectric detector (PD1, PD2, PD3 and PD4).

The user data (Data 1) were simulated and discussed to demonstrate the performance of the optical frequency-hopping system. As shown in Fig. 6, the BER performance and eye diagram of 25-Gb/s decrypted signals through back to back, 32-km SMF and 8-km DCF transmission were measured, and error-free results were achieved. Meanwhile, the dispersion coefficient of SMF and DCF is $16\times10^{-6}$ s/m$^2$ and is $-64\times10^{-6}$ s/m$^2$, respectively. In order to study whether the residual chromatic dispersion affect the feasibility of proposed communication system, the BER performance versus the received power at different dispersion coefficients of DCF has been measured. As shown in Fig. 7, although the residual chromatic dispersion will deteriorate the proposed system performance, the temperate residual chromatic dispersion is acceptable. In conclusion, the pro-

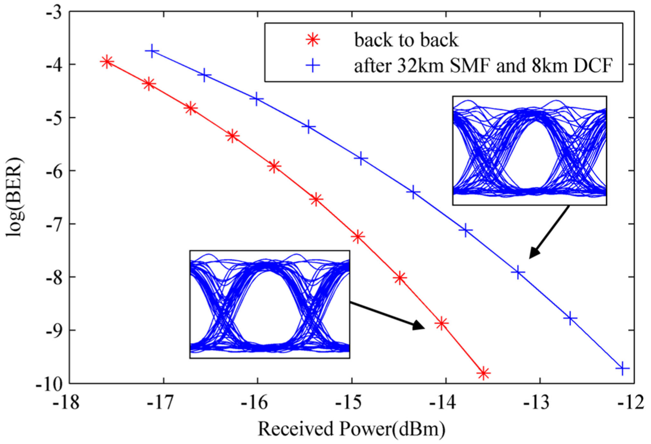


Fig. 6. The measured BER performance of decrypted signals.

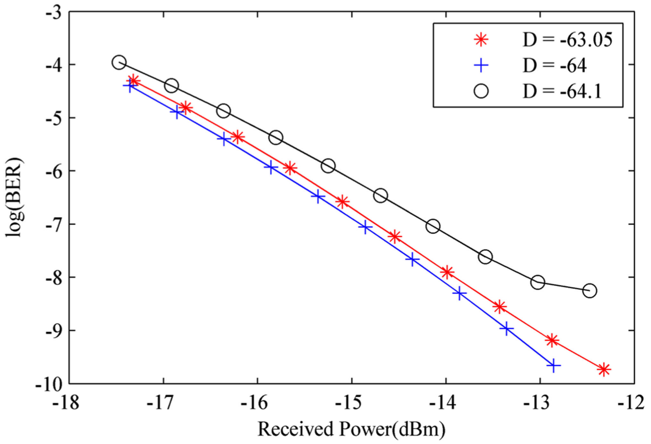


Fig. 7. The measured BER performance versus the received power at different dispersion coefficients of DCF. D: dispersion coefficients.

posed communication system is not only security, but simple and flexible due to the same unit in transmitter and receiver.

## 5. Conclusion

In this paper, a novel optical frequency-hopping scheme based on flexible structures for secure optical communications is proposed. Through fragmenting user data and modulating them onto different optical wavelengths, the security of optical communication system is greatly enhanced. The security of a four-wavelength-frequency-hopping system with 25-Gb/s bit rate and 25-Gb/s hopping rate through 32-km SMF and 8-km DCF transmission had been verified to be efficacious. In addition, the same unit which is used both in the transmitter and the receiver can reduce the cost of the security communication system and makes it more flexible.

## References

[1] K. Shaneman and S. Gray, “Optical network security: Technical analysis of fiber tapping mechanisms and methods for detection & prevention,” in *Proc. Int. Conf. IEEE Mil. Commun.*, Monterey, CA, USA, 2002, vol. 2, pp. 711–716.

[2] L. M. Keuthan, J. S. Sanghera, and I. D. Aggarwal, “Optical internet security,” *Proc. SPIE*, vol. 4738, pp. 150–156, 2002.

[3] B. Wu and E. Narimanov, “Secure stealth transmission over an existing public fiber-optical network,” in *Proc. Int. Conf. IEEE Opt. Fiber Commun. Nat. Fiber Opt. Eng.*, 2006, Paper OTuJ4.

[4] S. Tang and J. M. Liu, “Message encoding–decoding at 2.5 Gbits/s through synchronization of chaotic pulsing semiconductor lasers,” *Opt. Lett.*, vol. 26, pp. 1843–1845, 2001.

[5] J. Paul, M. W. Lee, and K. A. Shore, “3.5-GHz signal transmission in an all-optical chaotic communication scheme using 1550-nm diode lasers,” *IEEE Photon. Technol. Lett.*, vol. 17, no. 4, pp. 920–922, May 2005.

[6] Z. Jiang, D. E. Leaird, R. V. Roussev, C. Langrock, M. M. Fejer, and A. M. Weiner, “Four-user, 2.5-Gb/s, spectrally coded OCDMA system demonstration using low-power nonlinear processing,” *J. Lightw. Technol.*, vol. 23, no. 1, pp. 143–158, Jan. 2005.

[7] P. C. Teh, M. Ibsen, J. H. Lee, P. Petropoulos, and D. J. Richardson, “Demonstration of a four-channel WDM/OCDMA system using 255-chip, 320 Gchip/s quaternary phase coding gratings,” *IEEE Photon. Technol. Lett.*, vol. 14, no. 2, pp. 227–229, Feb. 2002.

[8] D. E. Leaird, Z. Jiang, and A. M. Weiner, “Experimental investigation of security issues in OCDMA: A code-switching scheme,” *Electron. Lett.*, vol. 41, no. 14, pp. 817–819, 2005.

[9] S. L. Wang, W. Chen, N. H. Zhu, J. G. Liu, W. T. Wang, and J. J. Guo, “A novel optical frequency-hopping scheme for secure WDM optical communications,” *IEEE Photon. J.*, vol. 7, no. 3, Jun. 2015, Art. no. 7201108.

[10] Q. Huang *et al.*, “Secure free-space optical communication system based on data fragmentation multipath transmission technology,” *Opt. Exp.*, vol. 26, pp. 13536–13542, 2018.

[11] L. Huo, J. Zhao, C. Lin, C.-K. Chan, and Z. Wang, “Demonstration of an optical frequency-hopping scheme for secure communications,” in *Proc. Int. Conf. Lasers Electro-Opt. Quantum Electron. Laser Sci.*, Long Beach, CA, USA, 2006, pp. 1–2.

[12] S.-S. Pun, C.-K. Chan, and L.-K. Chen, “A novel optical frequency-shift-keying transmitter based on polarization modulation,” *IEEE Photon. Technol. Lett.*, vol. 17, no. 7, pp. 1528–1530, Jul. 2005.

[13] W. Hung, N. Deng, C.-K. Chan, and L.-K. Chen, “A novel wavelength shift keying transmitter based on optical phase modulation,” *IEEE Photon. Technol. Lett.*, vol. 16, no. 7, pp. 1739–1741, Jul. 2004.

[14] C. Song, J. Liu, and B. Chen, “Wavelength remodulation by optical frequency-shift keying in WDM-PON,” in *Proc. Int. Symp. IEEE Photon. Optoelectron.*, Wuhan, China, 2009, pp. 1–4.

[15] B. Zhu *et al.*, “112-Tb/s (7×160×107Gb/s) space-division multiplexed DWDM transmission over a 76.8-km multicore fiber,” in *Proc. 37th Eur. Conf. Exhib. Opt. Commun.*, Geneva, Switzerland, 2011, pp. 1–3.